Common-Criteria-Dokument

Sicherheitsvorgaben EAL3+

Project	**Name:**	**CM3621 / CM3821**
	ID:	**CM3x21**
Zertifizierung	**ID:**	**BSI-DSZ-CC-0295**
Bestätigung	**ID:**	**BSI.02057.TE.xx.2005**
Dokument	**ID:**	**C2-ST-Sicherheitsvorgaben-V101.doc**
	Version:	**1.01**
	Status:	**Revised**
	Date:	**07.03.2005**
	Prepared by:	**Werner Waitz**
	Date/Signature:	**07.03.2005**
	Checked by:	**Christian Hintersteiner**
	Date/Signature:	**07.03.2005**

OMNIKEY AG
Sitz Walluf
Am Klingenweg 6a
D-65396 Walluf

Revision History

Date	Version	Description	Author
11.01.2005	1.00	First Draft	**Werner Waitz**
07.03.2005	1.01	Dummycode, Anmerkungen BSI vom 23.02.	**Werner Waitz**

Distribution List

Name	Company / Department	Notes
Hans-Werner Blißenbach	TÜVIT in Essen	Evaluierung
Peter Herrmann	TÜVIT in Essen	Evaluierung
Dr. Thomas Schöller	BSI Bonn	Zertifizierung
Sabine Weintauer	BSI Bonn	Zertifizierung
Werner Waitz	OMNIKEY AG	Engineering
Christian Hintersteiner	OMNIKEY AG	Engineering

Inhaltsverzeichnis

1. ST-Einführung „ASE_INT.1“

1.1 ST Identifikation

Titel:	Common-Criteria-Dokument Sicherheitsvorgaben EAL3+ für CM3621 / CM3821
Version:	1.01
Datum:	07.03.2005
Datei Name:	C2-ST-Sicherheitsvorgaben-V101.doc
Autor(en):	Werner Waitz
Zert. ID:	**BSI-DSZ-CC-0295**

Der Evaluationsgegenstand ist das Chipkartenterminal CM3621 / CM3821 (**TOE**=**T**arget **o**f **E**valuation) der Familie „CardMan Trust“ mit der Firmware-Version 6.00 des Herstellers OMNIKEY AG.

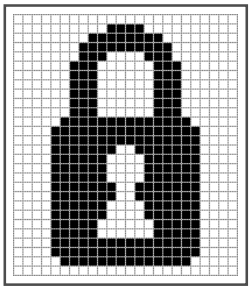
Der Evaluationsgegenstand unterteilt sich in folgende Produktvarianten:

Variante 1: CardMan® 3621

Abbildung 1: CardMan® 3621 R1.00

USB Trusted Smart Card Reader mit LED Anzeige, R1.00 = Common Criteria

Variante 2: CardMan® 3821



Sicheres Zeichen

Abbildung 2: CardMan® 3821 R1.00

USB Trusted Smart Card Reader mit 2-zeiligem LCD Display und SPE Zeichen, R1.00 = Common Criteria

In allen Produktvarianten ist die gleiche zu evaluierende Firmware 6.00 **enthalten.**

1.2 Erklärung der Sachnummern

Die Sachnummer besteht aus zwei Blöcken. Beispiel: CardMan 3621

Block1: CardMan geschütztes Warenzeichen der OMNIKEY AG für Smart Card Reader.

Block2: 3621 Produktnummer

```
3621
||||
|||+---  1 = Lesergeneration mit Atmel-Chip
||+----  2 = USB Interface
|+-----  6 = LED Anzeige + PIN-Pad
|        8 = LCD Display + PIN-Pad
+------  3 = Leserfamilie / Desktop mit EMV-Zertifikat
```

Block3: R1.00 kennzeichnet den Gerätestand (Versionsnummer) des Chipkartenterminals.

```
R1.00
 | |
 | +-- fortlaufende Geräteversionsnummer
 +-----  Klasse 2 mit Common Criteria
```

Der Gerätestand R1.00 entspricht der Firmware 6.00. Die Nummer hat nur indirekt mit der Firmware zu tun. Sie ist lediglich ein Zähler für den Stand des Chipkartenterminals (00, 01, …). Die genaue Zuordnung kann anhand der Entwicklungsdokumente nachvollzogen werden. Die Sachnummer inkl. Gerätestand ist auf der Rückseite des Chipkartenterminals und auf dem Verpackungskarton aufgebracht. Diese Nummer findet sich auch im Handbuch wieder.

1.3 ST Übersicht

Beim TOE handelt es sich um einen USB-Smart Card Reader mit PIN-Pad zur sicheren PIN-Eingabe.
Die Sicherheitsvorgaben stellen die funktionalen sowie organisatorischen Sicherheitsanforderungen und -prozeduren an den TOE und dessen Einsatzumgebung dar, die den Sicherheitszielen nach [SigG]/[SigV]

- Keine Preisgabe oder Speicherung der Identifikationsdaten (§15 Abs. 2 Nr. 1a [SigV])
- Erkennbarkeit sicherheitstechnischer Veränderungen (§15 Abs. 4 [SigV])

entsprechen.

1.4 Postulat der Übereinstimmung mit den [CC]

Die Sicherheitsvorgaben sind in ihren funktionalen Anforderungen konform zu den Vorgaben nach Teil 2 und in ihren Anforderungen zur Vertrauenswürdigkeit konform zu Teil 3 der [CC] (Version 2.1 August 1999) EAL3 mit Zusatz (ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4).

2. TOE-Beschreibung „ASE_DES.1“

Der TOE ist ein Smart Card Reader mit Tastatur und LCD- (LED-) Anzeige, im Folgenden „Kartenterminal“ genannt. Mit dem TOE können kontaktbehaftete Speicher- und Prozessorchipkarten verarbeitet werden. Die sichere PIN-Eingabe wird vom TOE nur für Prozessorchipkarten unterstützt. Die PIN wird über den Nummernblock des TOE eingegeben. Die Prozessorkarten müssen den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen und unterstützen die Übertragungsprotokolle T=0 und T=1. Bei synchronen Chipkarten basiert das Übertragungsprotokoll auf den herstellerspezifischen Spezifikationen.

Der TOE besteht somit aus Hardware- und Firmwareanteilen. Er kann an jedem USB-fähigen PC-System betrieben werden. Der TOE ist für den Einsatz im nichtöffentlichen („privaten“) Bereich vorgesehen. Hierzu zählt auch die normale Büroumgebung mit geregelten Zugriffsmöglichkeiten. Der TOE bietet Schutz gegen Angreifer mit hohem Angriffspotential. Der Benutzer ist zudem in der Lage und auch dazu angehalten, die Unversehrtheit des TOE zu überprüfen.

Zum Lieferumfang gehören:

- ***Smart Card Reader mit USB Kabel*** CM3621 / CM3821
- ***Bedienungsanleitung (Sicherheitshinweise)***

Darüber hinaus wird der TOE kundenspezifisch mit weiteren Komponenten ausgeliefert (z.B. Treiber-CD), die jedoch nicht zum TOE gehören und somit nicht Gegenstand der Evaluierung sind.

Die Schnittstelle zwischen Host und dem Kartenterminal basiert auf dem Funktionsumfang der [CCID]. Die USB-Schnittstelle stellt die physikalische und logische Abgrenzung des TOE zum Host-System dar. Ziel ist es das Kartenterminal u.a. für die Applikation „digitale Signatur“ nach dem deutschen Signaturgesetz [SigG] einzusetzen.

Um die PIN-Eingabe zu starten, wird von der Applikation das PIN-Eingabekommando an das Kartenterminal gesendet, welches anschließend in den Modus der sicheren PIN-Eingabe umschaltet. Optisch wird dies dem Nutzer über die rot blinkende LED oder das Aufleuchten des sicheren Zeichens im Display, signalisiert. Nach erfolgreicher Eingabe der PIN wird diese direkt zur Chipkarte gesendet und anschließend wieder in den Idle-Mode zurückgekehrt. Die PIN wird nur zur Chipkarte hin übertragen.

Der Eingabefortschritt wird bei beiden CardMan-Varianten mittels der Übertragung von Dummycodes [*] dem System mitgeteilt. Bei der Variante mit LCD-Display wird der Eingabefortschritt zusätzlich im Display mit ~~Dummycodes~~Sternchen [*] dargestellt.
Somit werden Eingaben im sicheren Modus (bei rot blinkender LED oder Anzeige des sicheren Zeichens) immer nur zur Chipkarte und niemals zum PC-System übertragen.

In der nachfolgenden Tabelle sind die Funktionen aufgeführt, die durch verschiedene Tasten ausgeführt werden können:

Tabelle 1: Tastenbelegung des Kartenterminals

Darstellung des Tastenfeldes	Zeichen	Funktion	Farbe
	**F * .**	ohne Funktion	Graue Taste
	0 1 2 3 4 5 6 7 8 9	Zifferntasten zur PIN-Eingabe	Graue Taste
	✖	Abbruch	Rote Taste
	←	Backspace	Gelbe Taste

	✓	Eingabebestätigung	Grüne Taste

Die PIN wird nur zur Chipkarte übertragen beziehungsweise abgefragt, wenn:

- das richtige CT-Commando nach [CCID],
- das richtige Chipkartenkommando nach [ISO 7816] und [EMV 2000]

vorhanden ist.

Um sicherheitstechnische Veränderungen am Kartenterminal durch den Nutzer zu erkennen, wird am Kartenterminal über der Trennkante zwischen Gehäuseober- und Unterteil ein authentisches und fälschungssicheres Siegel aufgebracht, welches gewährleistet, dass ein Öffnen des Gehäuses ohne Beschädigung der Siegel nicht möglich ist. Um den Nutzer auf die Unversehrtheit aufmerksam zu machen, wird er in der Bedienungsanleitung explizit darauf hingewiesen. Dem Nutzer werden dort das Aussehen (Abbildung), die Beschaffenheit und die Position der Siegel beschrieben.

Das Kartenterminal wird über die USB-Schnittstelle mit der erforderlichen Betriebsspannung (+5 Volt) versorgt. Somit ist bei nicht eingeschaltetem Host keine Funktionalität im Kartenterminal zu erreichen.

Die Kommunikation des Kartenterminals basiert auf dem von Microsoft spezifizierten PC/SC-Standard, welcher Bestandteil der heute am Markt verfügbaren Betriebssysteme (wie z.B. Windows XP / 2000, Linux-Derivate) ist.

Die Treibersoftware gehört nicht zum Evaluationsumfang.

3. TOE-Sicherheitsumgebung „ASE_ENV.1“

Im folgenden Kapitel wird die Sicherheitsumgebung, in der der TOE eingesetzt werden soll, dargelegt. Dies umfasst die Sicherheitsaspekte der Umgebung, sowie die erwartete Art des Gebrauchs des TOE. In diesem Zusammenhang werden die zu schützenden Werte und die handelnden Personen in Hinblick auf gebrauchsgerechte und missbräuchliche Nutzung des TOE beleuchtet.

Zu schützen sind die PIN als Identifikationsmerkmal des Chipkarteninhabers, sowie die Firmware und Hardware des TOE.

Als Bedrohungen für den TOE durch einen Angreifer gelten das Ausspähen der Identifikationsdaten und die sicherheitstechnische Veränderung am TOE.

Um diesen Bedrohungen entgegen zu wirken, wurden entsprechende Mechanismen integriert:

- Die sichere PIN-Eingabe wird durch eine LED beziehungsweise durch ein sicheres Zeichen im LCD-Display angezeigt,
- Speicherbereiche werden definiert aufbereitet,
- Der TOE darf die PIN nur zur Chipkarte übertragen,
- Die PIN darf nur über zugelassene PIN-Kommandos an die Chipkarte weitergegeben werden,
- Der TOE wird durch Siegel geschützt,
- Der Endanwender wird über seine Verantwortung während der Nutzung des TOEs informiert.

3.1 Annahmen

Der TOE ist für einen universellen Einsatz in chipkartenbasierenden Applikationen ohne vorherige Authentisierung geeignet. Mögliche Anwendungen sind:

- Digitale Signatur
- Homebanking (HBCI)
- Access Control (PC-Systeme)
- Internet Shopping

Bei der Anwendung qualifizierte elektronische Signatur dürfen ausschließlich im Sinne des SigG und SigV bestätigte Chipkarten und bestätigte Signaturanwendungsprogramme beziehungsweise herstellererklärte Signuaturanwendungsprogramme verwendet werden.
Zugelassene Komponenten sind auf der Internetseite der RegTP zu finden.
Die Sicherheitsfunktionalität des EVG ist unabhängig vom ansteuernden Anwendungsprogramm immer wirksam. Um die sichere PIN-Eingabe zu nutzen, ist lediglich das entsprechende CT-Commando nach [CCID] zu verwenden. Die Chipkarten müssen die Voraussetzungen nach AE.2 erfüllen.

Der Einsatz des Kartenterminal ist für folgende **nichtöffentliche** Umgebungen zugelassen:

- Single- und MultiUser-PC im privaten Bereich und in der Büroumgebung.

Unter nichtöffentlicher Umgebung fallen alle Bereiche, die nicht für die Allgemeinheit (Öffentlichkeit) zugänglich sind.

Der Endanwender wird über seine Verantwortung während der Nutzung des TOEs informiert.
Die Regeln zur sicheren Aufbewahrung und Nichtweitergabe der PIN werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt.

Tabelle 2: Annahmen

Annahmen	Beschreibung
AE.1	Es wird angenommen, dass der TOE für die nicht öffentliche Umgebung eingesetzt wird.
AE.2	Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen.
AE.3	Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme und regelmäßig vor Benutzung des Gerätes durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheits-technischen Veränderungen am Kartenterminal vorgenommen wurden.
AE.4	Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet.
AE.5	Es wird angenommen, dass der Benutzer während der PIN-Eingabe den Status der LED beziehungsweise das LCD-Display dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.

3.2 Bedrohungen

Es werden folgende Bedrohungen angenommen.

Tabelle 3: Bedrohungen

Bedrohungen	Beschreibung
T.1	Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den TOE eingegebene PIN auszuspähen.
T.2	Ein Angreifer könnte versuchen, eine PIN-Eingabe zu provozieren und damit die PIN zu erlangen.
T.3a	Ein Angreifer könnte versuchen, den TOE in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln.
T.3b	Ein Angreifer könnte versuchen, die im TOE zwischengespeicherte PIN auszulesen.
T.4	Ein Angreifer könnte versuchen, die PIN in einen ungeschützten Bereich der Chipkarte zu schreiben, um sie anschließend daraus auszulesen
T.5	Ein Angreifer könnte versuchen, das Sicherheitssiegels zu manipulieren, um sicherheitstechnische Veränderungen am TOE zu verschleiern.

3.3 Organisatorische Sicherheitspolitik

Es sind keine organisatorischen Sicherheitspolitiken vorgesehen.

4. Sicherheitsziele „ASE_OBJ.1“

In diesem Kapitel werden die Sicherheitsziele für den TOE und dessen Umgebung definiert. Mit den folgenden Sicherheitszielen wird allen identifizierten Bedrohungen entgegengewirkt und die Annahmen abgedeckt.
Im Kapitel 4.1 werden die Sicherheitsziele für den TOE definiert, während in Kapitel 4.2 die Sicherheitsziele für die Umgebung des TOE festgelegt werden.
Im Kapitel 4.3 werden die Zusammenhänge zwischen Anforderungen von [SigG]/[SigV] und den Sicherheitszielen der [CC] darstellt.

4.1 Sicherheitsziele für den TOE

Die Sicherheitsziele für den TOE sind in der nachfolgenden Tabelle aufgeführt.

Tabelle 4: Sicherheitsziele für den TOE

Sicherheitsziele für den TOE	Beschreibung
O.1	Der TOE stellt sicher, dass die PIN, außer zum Zeitpunkt der Verarbeitung, nicht gespeichert wird.
O.2	Der TOE stellt sicher, dass dem Anwender die sichere PIN-Eingabe eindeutig signalisiert wird.
O.3	Der TOE stellt sicher, dass die PIN nur zur Chipkarte übertragen wird.
O.4	Der TOE stellt sicher, dass die PIN nur über PIN-Kommandos mit zulässigen Instructionsbytes an die Chipkarte weitergeleitet wird.
O.5	Der TOE stellt sicher, dass sicherheitstechnische Veränderungen am TOE durch das Sicherheitssiegel erkennbar sind.

4.2 Sicherheitsziele für die Umgebung

Die Regeln zur sicheren Aufbewahrung und Nichtweitergabe der PIN werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt.
Der Endanwender muss über seine Verantwortung während der Nutzung des TOEs informiert werden.
Die Sicherheitsziele für die Umgebung werden in Tabelle 5 definiert.

Tabelle 5: Sicherheitsziele für die Umgebung

Sicherheitsziele für die Umgebung	Beschreibung
OE.1	Der TOE darf nur in nicht öffentlicher Umgebung eingesetzt werden.
OE.2	Der Anwender darf ausschließlich Prozessorkarten benutzen, die den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen.
OE.3	Der Anwender muss das Sicherheitssiegel (Siegelaufdruck~~nummer~~) regelmäßig vor Benutzung des Gerätes auf Unversehrtheit prüfen.
OE.4	Eine unbeobachtete Eingabe der Identifikationsdaten (PIN) ist durch den Benutzer zu gewährleisten.
OE.5	Während der PIN-Eingabe muss der Benutzer den Status der LEDs beziehungsweise des LCD-Displays dahingehend überprüfen, dass der Modus der sicheren PIN-Eingabe aktiv ist.

4.3 Zusammenhänge: Anforderungen [SigG]/[SigV] - Sicherheitsziele

In der nachfolgenden Tabelle werden die in [SigG]/[SigV] geforderten Sicherheitsanforderungen den Sicherheitszielen der Common Criteria zugeordnet.

Tabelle 6: Zuordnung der Sicherheitsziele: [SigG]/[SigV] - Common Criteria

Gesetz / Verordnung	**Gesetzestext**	**Sicher-heitsziel**	**Beschreibung**
§15 Abs. 4 [SigV]	Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar sein	O.5 OE.3	Sicherheitstechnische Veränderungen am TOE müssen durch das Sicherheitssiegel erkennbar sein. Der Anwender muss das Sicherheitssiegel (Siegelaufdrucknummer) regelmäßig vor Benutzung des Gerätes auf Unversehrtheit prüfen.
§15 Abs. 2 Nr. 1a [SigV]	Signaturanwendungskomponenten nach §17 Abs. 2 des [SigG] müssen gewährleisten, dass bei der Erzeugung einer qualifizierten Signatur die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden	O.1 O.2 O.3 O.4 OE.5	Die PIN wird außer zum Zeitpunkt der Verarbeitung vom TOE nicht gespeichert. Der TOE stellt sicher, daß dem Anwender die sichere PIN-Eingabe eindeutig signalisiert wird. Der TOE stellt sicher, daß die PIN nur zur Chipkarte übertragen wird. Der TOE stellt sicher, daß die PIN nur über PIN-Kommandos mit zulässigen Instructionsbytes an die Chipkarte weitergeleitet wird. Während der PIN-Eingabe muß der Benutzer den Status der LEDs beziehungsweise des Displays dahingehend überprüfen, dass der Modus der sicheren PIN-Eingabe aktiv ist.

5. IT-Sicherheitsanforderungen „ASE_REQ.1“

Dieses Kapitel beschreibt die TOE-Sicherheitsanforderungen in den Teilkapitel 5.1 Funktionale Sicherheitsanforderungen an den TOE, 5.2 Anforderungen an die Mindeststärke der TOE-Sicherheitsfunktionen, 5.3 Anforderungen an die Vertrauenswürdigkeit des TOE und 5.4 Sicherheitsanforderungen an die IT-Umgebung.

5.1 Funktionale Sicherheitsanforderungen an den TOE

In der nachfolgenden Tabelle sind alle funktionalen Anforderungen an den TOE in Form von Verweisen auf Komponenten der Common Criteria Teil 2 [CC] aufgeführt. In der vierten Spalte sind die Abhängigkeiten zwischen funktionalen Komponenten aufgeführt. ~~So weit als möglich wurde~~ ~~d~~Die Ausführung der Operationen, Auswahl und Zuweisung ist durch kursive Schrift im Text der Komponenten gekennzeichnet.

Tabelle 7: Funktionale Anforderungen an den TOE

Nr.	ID	Klasse / Komponente	Abhängigkeiten
	FDP	**Schutz der Benutzerdaten**	
1	FDP_ACC.1	Teilweise Zugriffskontrolle	FDP_ACF.1
2	FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACC.1 FMT_MSA.3
3	FDP_RIP.2	Vollständiger Schutz bei erhalten gebliebenen Informationen	Keine
	FTA	**TOE-Zugriff**	
4	FTA_TAB.1	TOE-Zugriffswarnmeldung	Keine
	FPT	**Schutz der TSF**	
5	FPT_PHP.1	Passive Erkennung materieller Angriffe	FMT_MOF.1

5.1.1 Schutz der Benutzerdaten (Klasse FDP)

5.1.1.1 Zugriffskontrollpolitik (Familie FDP_ACC)

FDP_ACC.1 Teilweise Zugriffskontrolle

Die TSP legt die Regeln fest, nach denen der TOE den Zugriff auf seine Betriebsmittel und somit alle durch den TOE kontrollierten Informationen und Dienste steuert.
Die Chipkarten-Zugriffspolitik, die den Schutz der PIN regelt, wird durch die Sicherheitsfunktionen durchgesetzt.
Die TSF müssen die *Chipkartenleser-Zugriffspolitik* für
die Subjekte:

- *Benutzer über die PIN-Pad-Schnittstelle*
- *PC über USB-Schnittstelle*
- *Chipkarte über Kartenleserschnittstelle*

die Objekte:

- *PIN*
- *LED oder LCD-Display zur Anzeige der sicheren PIN-Eingabe*

und die durch die Chipkartenleser-Zugriffspolitik abgedeckten Operationen:

- *PIN-Eingabe*
- *Übermittlung der PIN*
- *Ansteuerung der LED beziehungsweise Darstellung des sicheren Zeichens im LCD-Display*

durchsetzen.

5.1.1.2 Zugriffskontrollfunktionen (Familie FDP_ACF)

FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

FDP_ACF.1.1:

Die TSF müssen die *Chipkartenleser-Zugriffspolitik* für Objekte, die auf *der Identität des Objektes* basieren, durchsetzen.

Da alle Objekte ausschließlich über definierte Schnittstellen des TOE erreichbar sind und pro Schnittstelle jeweils ein Subjekt definiert ist, ist die Identität der Objekte als Sicherheitsattribut ausreichend.
Die Subjekte sind:

- *Benutzer über die PIN-Pad-Schnittstelle*
- *PC über USB-Schnittstelle*
- *Chipkarte über Kartenleserschnittstelle*

Die Objekte sind:

- *PIN*
- *LED oder LCD-Display zur Anzeige der sicheren PIN-Eingabe*

Die Operationen sind:

- *PIN-Eingabe*
- *Übermittlung der PIN*
- *Ansteuerung der LED beziehungsweise Darstellung des sicheren Zeichens im LCD-Display*

FDP_ACF.1.2:

Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:

Von einer Applikation sendet der PC (Subjekt) über die USB-Schnittstelle ein explizites Kommando an den Kartenleser, wodurch die LED beziehungsweise das sichere Zeichen (Objekt) zur Anzeige des sicheren Eingabemodus vom TOE angesteuert (Operation) und die eingegebene PIN (Objekt) vom TOE an die Chipkarte (Subjekt) übermittelt (Operation) wird wenn,
das Kommando der Kommandostruktur gemäß [CCID] entspricht (Verifizieren und Modifizieren) und zusätzlich
die an die Chipkarte weiterzuleitende Instruktion einem der folgenden Instruktionbytes entspricht:

- *VERIFY (ISO/IEC 7816-4)* $INS=20_h$
- *CHANGE REFERENCE DATA (ISO/IEC 7816-8)* $INS=24_h$
- *DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8)* $INS=26_h$
- *ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8)* $INS=28_h$
- *RESET RETRY COUNTER (ISO/IEC 7816-8)* $INS=2C_h$

Die PIN (Objekt) kann vom Benutzer (Subjekt) über das PIN-Pad des Kartenterminals eingegeben (Operation) werden.

Der TOE darf die PIN (Objekt) nur über die Kartenleserschnittstelle zur Chipkarte (Subjekt) übermitteln (Operation).

FDP_ACF.1.3

Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf den folgenden zusätzlichen Regeln, explizit autorisieren:
Die TSF müssen hierbei keine zusätzlichen Regeln berücksichtigen.

FDP_ACF.1.4

Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf *keinen zusätzlichen Regeln*, explizit verweigern.

5.1.1.3 Schutz bei erhalten gebliebenen Informationen (Familie FDP_RIP)

FDP_RIP.2 Vollständiger Schutz bei erhalten gebliebenen Informationen

FDP_RIP.2.1

Die TSF müssen sicherstellen, dass der frühere Informationsinhalt eines Betriebsmittels bei *Wiederfreigabe eines Betriebsmittels von* allen Objekten nicht verfügbar ist.

Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos zur Chipkarte beziehungsweise dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED beziehungsweise das sichere Zeichen zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.
Die Speicheraufbereitung stellt sicher, dass keine persönlichen Identifikationsdaten beziehungsweise Datenfragmente im Kartenterminal nach Abschluss der PIN-Eingabe oder Entnahme der Karte vorhanden sind.
Das Ausschalten der LED beziehungsweise des sicheren Zeichens zur Anzeige der sicheren PIN-Eingabe stellt sicher, dass dieses Objekt nicht missbräuchlich genutzt werden kann, um beispielsweise eine PIN-Eingabe zu provozieren.

5.1.2 TOE-Zugriff (Klasse FTA)

5.1.2.1 TOE-Zugriffswarnmeldung (Familie FTA_TAB)

FTA_TAB.1 Vorgegebene TOE-Zugriffswarnmeldung

FTA_TAB.1.1

Vor Einrichtung einer Benutzersitzung müssen die TSF einen beratenden Warnhinweis für den nichtautorisierten Gebrauch des TOE anzeigen.

Während sich der TOE Variante CM3621 im sicheren Eingabemodus befindet, wird dieser Zustand durch eine rotblinkende LED angezeigt, die nach Beendigung wieder erlischt.
Während sich der TOE Variante CM3821 im sicheren Eingabemodus befindet, wird dieser Zustand durch ein sicheres Zeichen im LCD-Display angezeigt, welches nach Beendigung wieder erlischt.

5.1.3 Schutz der TSF (Klasse FPT)

5.1.3.1 Materieller TSF-Schutz (Familie FPT_PHP)

FPT_PHP.1 Passive Erkennung materieller Angriffe

FPT_PHP.1.1

Die TSF müssen materielle Manipulationen, die die TSF bloßstellen können, eindeutig erkennen.

Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden.

FPT_PHP.1.2

Die TSF müssen die Fähigkeit zum Feststellen erfolgter materieller Manipulationen der TSF-Geräte oder TSF-Elemente bereitstellen.

Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann.

5.2 Anforderungen an die Mindeststärke der TOE-Sicherheitsfunktionen

Der TOE bietet Schutz gegen hohes Angriffspotential. Die geforderte Mindeststärke des TOE ist „hoch“.

~~Für den TOE gelten keine funktionalen Sicherheitsanforderungen, die für eine Betrachtung der Stärke (SOF) in Frage kommen.~~

5.3 Anforderungen an die Vertrauenswürdigkeit des TOE

Der TOE soll die Vertrauenswürdigkeitsanforderungen entsprechend der Klasse ASE und der Vertrauenswürdigkeitsstufe EAL3 gemäß Teil 3 der [CC] mit Zusatz ADO_DEL.2, ADV_IMP.1, ADV_LLD.1 , ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 erfüllen. Die Widerstandsfähigkeit des TOE gegen Angreifer mit hohem Angriffpotential wird mit hoch eingestuft. Alle Anforderungen der Evaluationsstufe EAL3+ sind in der folgenden Tabelle aufgelistet. Die zusätzlichen Anforderungen für die Einstufung mit Zusatz sind fettgedruckt. Die Punkte AVA_MSU.1 und AVA_VLA.1 werden durch AVA_MSU.3 und AVA_VLA.4 ersetzt.

Tabelle 8 Anforderungen an die Vertrauenswürdigkeit (ASE und EAL3+)

Vertrauenswürdig-keitsklasse	Vertrauenswürdig-keitsfamilie	Vertrauenswürdigkeitskomponenten
Evaluation der Sicherheitsvorgaben	ASE_DES.1	Beschreibung des TOE
	ASE_ENV.1	Sicherheitsumgebung
	ASE_INT.1	ST Einführung
	ASE_OBJ.1	Sicherheitsziele
	ASE_PPC.1	PP-Postulate
	ASE_REQ.1	IT – Sicherheitsanforderungen
	ASE_SRE.1	Explizit dargelegte IT – Sicherheitsanforderungen
	ASE_TSS.1	TOE – Übersichtsspezifikation
Konfigurations-management	ACM_CAP.3	Autorisierungskontrolle
	ACM_SCP.1	TOE – CM – Umfang
Auslieferung und Betrieb	**ADO_DEL.2**	**Erkennung von Modifizierungen**
	ADO_IGS.1	Installations-, Generierungs-, und Anlaufprozeduren
Entwicklung	ADV_FSP.1	Informell funktionale Spezifikation
	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
	ADV_IMP.1	**Teilmenge der Implementierung der TSF**
	ADV_LLD.1	**Beschreibender Entwurf auf niedriger Ebene**
	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1	Systemverwalterhandbuch
	AGD_USR.1	Benutzerhandbuch
Lebenszyklus – Unterstützung	ALC_DVS.1	Identifikation der Sicherheitsmaßnahmen
	ALC_TAT.1	**Klar festgelegte Entwicklungswerkzeuge**
Testen	ATE_COV.2	Analyse der Testabdeckung
	ATE_DPT.1	Testen – Entwurf auf hoher Ebene
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen – Stichprobenartig
Schwachstellen-bewertung	**AVA_MSU.3**	**Analysieren und Testen auf unsichere Zustände**
	AVA_SOF.1	Stärke der TOE-Sicherheitsfunktionen
	AVA_VLA.4	**Hohe Widerstandsfähigkeit**

5.4 Sicherheitsanforderungen an die IT-Umgebung

Es gibt keine Sicherheitsanforderungen an die IT-Umgebung.

6. TOE-Übersichtsspezifikation „ASE_TSS.1“

Dieses Kapitel beschreibt im Unterkapitel 6.1 die TOE-Sicherheitsfunktionen sowie die in 6.2 beschriebene TOE-Sicherheitsmaßnahme Versiegelung. Die vom Entwickler ergriffenen Maßnahmen zur Vertrauenswürdigkeit werden im Unterkapitel 6.3 aufgeführt.

6.1 TOE-Sicherheitsfunktionen

Um ein elektronisches Dokument digital zu signieren, wird der Benutzer durch die Applikation zum Stecken seiner Signaturkarte aufgefordert. Anschließend muss die Applikation "digitale Signatur" in der Chipkarte aktiviert werden. Hierzu muss sich der Inhaber durch Besitz (Signaturkarte) und Wissen (PIN) gegenüber seiner Signaturkarte authentifizieren.
Der Schutz der persönlichen Identifikationsdaten (PIN) steht im Vordergrund.

Der TOE bietet dem Nutzer die Sicherheitsfunktionen zum Schutz der Identifikationsdaten (PIN) und zur Wiederaufbereitung von Informationsträgern (Speicherbereiche und LED- beziehungsweise LCD-Anzeige).
Die Realisierung der einzelnen Sicherheitsfunktionen wird im Folgenden beschrieben.

Security Function 1: Speicherwiederaufbereitung (SF.1)

Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß [CCID] auf den sogenannten APDU’s. Wird eine APDU über die USB-Schnittstelle im Kartenterminal empfangen, so wird sie zuerst zwischengespeichert, um anschließend zur Chipkarte gesendet zu werden. Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos beziehungsweise dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, dass keine persönlichen Identifikationsdaten beziehungsweise Datenfragmente im Kartenterminal erhalten bleiben. Außerdem wird die LED beziehungsweise das sichere Zeichen zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.

Ein Angreifer mit hohem Angriffspotential kann diese Sicherheitsfunktion nicht umgehen, da er aufgrund der Implementierung dieser Funktion keine Möglichkeit besitzt, die Speicherwiederaufbereitung im TOE zu manipulieren.

Security Function 2: Schutz der PIN (SF.2)

Das Umschalten des Kartenterminals in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach [CCID] durchgeführt. Dieses CT-Kommando enthält die PIN-Handlingsvereinbarungen und das Chipkartenkommando, in welches die PIN an die spezifizierte Stelle integriert wird. Anhand des Instructionbytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN-Kommando handelt, welches explizit eine PIN-Eingabe erwartet. In der folgenden Tabelle sind die zugelassenen Instructionbytes aufgeführt.

Tabelle 9: Instructionbytes [ISO 7816]/[EMV 2000]

INS-Byte:	Bezeichnung:	Bedeutung	Norm:
20_h	VERIFY	PIN-Eingabe	ISO/IEC 7816-4
24_h	CHANGE REFERENCE DATA	PIN ändern	ISO/IEC 7816-8
26_h	DISABLE VERIFICATION REQUIREMENT	PIN aktivieren	ISO/IEC 7816-8
28_h	ENABLE VERIFICATION REQUIREMENT	PIN deaktivieren	ISO/IEC 7816-8
$2C_h$	RESET RETRY COUNTER	PIN entsperren	ISO/IEC 7816-8

Durch Umschalten des Kartenterminals in den PIN-Eingabemodus wird die Eingabe der persönlichen Identifikationsdaten im RAM zwischengespeichert, um sie nach Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden. Der PIN-Eingabemodus wird optisch durch ein rotes Blinken der SPE-LED beziehungsweise das Aufleuchten des sicheren Zeichens im Display angezeigt, bis die Vollständigkeit der PIN erreicht ist, beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit.
Der Eingabefortschritt wird mittels der Übertragung von Dummycodes ~~[*]~~ dem System mitgeteilt. Bei der Variante mit LCD-Display wird der Eingabefortschritt zusätzlich im Display mit ~~Dummycodes~~Sternchen [*] dargestellt.
Auch ein Angreifer mit hohem Angriffspotential kann die Sicherheitsfunktionen nicht manipulieren, da der Austausch der PIN nur zwischen Chipkarte und TOE über die Kartenleserschnittstelle erfolgt. Diese befindet sich im TOE und wird gegen Manipulation mit Sicherheitssiegel geschützt.

6.2 TOE-Sicherheitsmaßnahme Versiegelung (SM.1)

Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist.
Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Das eingesetzte Siegel ist fälschungssicher, weist Authentizitätsmerkmale auf und erfüllt die Sicherheitsstufe 2 entsprechend der BSI 7500 Druckschrift „Produkte für die materielle Sicherheit“ [BSI 7500].

6.3 Maßnahmen zur Vertrauenswürdigkeit

Der TOE erfüllt die Vertrauenswürdigkeitsanforderungen, die in der Klasse ASE und der Evaluationsstufe EAL3+ gefordert sind. Das vorliegende Dokument „Sicherheitsvorgaben“ dient der Erfüllung der Anforderungen entsprechend ASE. Neben dem TOE (gemäß ATE_IND.1) liefert der Hersteller im Rahmen der Evaluierung die folgenden zusätzlichen Dokumente, um eindeutig die Erfüllung der Anforderungen entsprechend EAL3+ nachzuweisen.

- Dokumentation Konfigurationsmanagement (gemäß ACM_CAP.3 und ACM_SCP.1)
- Dokumentation Auslieferung und Betrieb (gemäß ADO_DEL.2 und ADO_IGS.1)
- Dokumentation Entwicklung
  (gemäß ADV_FSP.1; ADV_HLD.2; ADV_IMP.1; ADV_LLD.1, ADV_RCR.1)
- Dokumentation Handbücher (gemäß AGD_ADM.1 und AGD_USR.1)
- Dokumentation Lebenszyklus-Unterstützung (gemäß ALC_DVS.1; ALC_TAT.1)
- Testdokumentation (gemäß ATE_COV.2; ATE_DPT.1; ATE_FUN.1)
- Dokumentation Schwachstellenbewertung
  (gemäß AVA_MSU.3; AVA_SOF.1; AVA_VLA.4)

7. PP-Postulate „ASE_PPC.1“

Es ist keine Konformität zu einem PP vorgesehen.

8. Erklärung

Dieses Kapitel enthält im Teilkapitel 8.1 die Erklärung der Sicherheitsziele, im Teilkapitel 8.2 die Erklärung der Sicherheitsanforderungen, im Teilkapitel 8.3 die Erklärung der TOE-Übersichtsspezifikation und im Teilkapitel 8.4 die Erklärung der PP-Postulate.

8.1 Erklärung der Sicherheitsziele

Dieses Kapitel erbringt den Nachweis, dass die dargelegten Sicherheitsziele auf alle Aspekte, die in der TOE-Sicherheitsumgebung identifiziert wurden, zurückverfolgbar und geeignet sind diese abzudecken.

Der TOE erfüllt die Anforderungen nach §15 Absatz 2 Nr.1a (keine Preisgabe oder Speicherung der Identifikationsdaten) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

In der nachfolgenden Tabelle wird die Zielrichtung für die einzelnen Sicherheitsziele aufgezeigt. Für jedes Sicherheitsziel für den TOE und für die Umgebung wird angegeben, welche Bedrohungen abgewehrt und welche Annahmen berücksichtigt werden sollen.

Tabelle 10: Annahmen/Bedrohungen vs. Sicherheitsziele

	O.1	O.2	O.3	O.4	O.5	OE.1	OE.2	OE.3	OE.4	OE.5
T.1			X		X	X		X		
T.2		X								X
T.3a					X	X		X		
T.3b	X				X			X		
T.4				X			X			
T.5					X	X		X		
AE.1						X				
AE.2							X			
AE.3								X		
AE.4									X	
AE.5										X

Aus der Tabelle ist ersichtlich, dass jede Bedrohung und jede Annahme von mindestens einem Sicherheitsziel adressiert wird und jedes Sicherheitsziel mindestens eine Bedrohung oder eine Annahme adressiert.
In der nachfolgenden Beschreibung wird aufgezeigt, in welcher Weise die Sicherheitsziele dazu beitragen, die aufgeführten Bedrohungen abzuwehren und in welcher Weise die aufgeführten Annahmen berücksichtigt werden.

8.1.1 Abwehr der Bedrohungen durch den TOE

In Tabelle 11 ist die Abwehr der einzelnen Bedrohungen durch den TOE aufgeführt.

Tabelle 11: Bedrohungen durch den TOE

T.1	Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den TOE eingegebene PIN auszuspähen.	
	O.3	Unterstützt die Abwehr der Bedrohung T.1, da die PIN nur zur Chipkarte hin übertragen wird und somit ein ausspähen verhindert.
	O.5	Unterstützt zusätzlich das Sicherheitsziel O.3 bei der Abwehr der Bedrohung T.1, indem sicherheitstechnische Veränderungen am TOE über das Siegel erkannt werden.
	OE.3	Unterstützt zusätzlich das Sicherheitsziel O.5 bei der Abwehr der Bedrohung T.1, da der Anwender das Sicherheitssiegel regelmäßig vor Benutzung auf Unversehrtheit prüfen muss.
	OE.1	Unterstützt zusätzlich das Sicherheitsziel O.5 und OE.3 bei der Abwehr der Bedrohung T.1, da der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird.
T.2	Ein Angreifer könnte versuchen, eine PIN-Eingabe zu provozieren und damit die PIN zu erlangen.	
	O.2	Unterstützt die Abwehr der Bedrohung T.2, da dem Anwender die sichere PIN-Eingabe durch eine blinkende LED beziehungsweise das sichere Zeichen im Display angezeigt wird.
	OE.5	Unterstützt zusätzlich die Abwehr der Bedrohung T.2, da der Anwender die Anzeige (LED, LCD-Display) zur sicheren PIN-Eingabe überprüft.
T.3a	Ein Angreifer könnte versuchen, den TOE in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln.	
	O.5	Unterstützt die Abwehr der Bedrohung T.3a, da sicherheitstechnische Veränderungen am TOE über das Siegel erkannt werden
	OE.3	Unterstützt zusätzlich das Sicherheitsziel O.5 bei der Abwehr der Bedrohung T.3a, da der Anwender das Sicherheitssiegel regelmäßig vor Benutzung auf Unversehrtheit prüfen muss.
	OE.1	Unterstützt zusätzlich das Sicherheitsziel O.5 und OE.3 bei der Abwehr der Bedrohung T.3a, da der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird.
T.3b	Ein Angreifer könnte versuchen, die im TOE zwischengespeicherte PIN auszulesen.	
	O.1	Unterstützt die Abwehr der Bedrohung T.3b, da die PIN außer zum Zeitpunkt der Verarbeitung vom TOE nicht gespeichert werden darf.
	O.5	Unterstützt zusätzlich das Sicherheitsziel O.1 bei der Abwehr der Bedrohung T.3b, indem sicherheitstechnische Veränderungen am TOE über das Siegel erkannt werden.
	OE.3	Unterstützt zusätzlich das Sicherheitsziel O.5 bei der Abwehr der Bedrohung T.3b, da der Anwender das Sicherheitssiegel regelmäßig vor Benutzung auf Unversehrtheit prüfen muss.
T.4	Ein Angreifer könnte versuchen, die PIN in einen ungeschützten Bereich der Chipkarte zu schreiben, um sie anschließend daraus auszulesen.	
	O.4	Unterstützt die Abwehr der Bedrohung T.4, da der TOE die PIN-Kommandos nur mit zulässigen Instructionsbytes an die Chipkarte weiterleiten darf und somit ein Speicherbefehl nicht ausgeführt wird.

	OE.2	Unterstützt zusätzlich das Sicherheitsziel O.4 bei der Abwehr der Bedrohung T.4, da durch die ausschließliche Verwendung von Prozessorkarten, die den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen, gewährleistet wird, dass die zulässigen Instructionbytes nicht zum Speichern auf der Chipkarte dienen.
T.5	Ein Angreifer könnte versuchen, durch Manipulation des Sicherheitssiegels sicherheitstechnische Veränderungen am TOE vorzunehmen.	
	O.5	Unterstützt die Abwehr der Bedrohung T.5, indem sicherheitstechnische Veränderungen am TOE über das Siegel erkannt werden
	OE.3	Unterstützt zusätzlich das Sicherheitsziel O.5 bei der Abwehr der Bedrohung T.5, da der Anwender das Sicherheitssiegel regelmäßig vor Benutzung auf Unversehrtheit prüfen muss.
	OE.1	Unterstützt zusätzlich das Sicherheitsziel O.5 und OE.3 bei der Abwehr der Bedrohung T.5, da der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird.

8.1.2 Berücksichtigung der Annahmen

Tabelle 12: Berücksichtigung der Annahmen

AE.1	Es wird angenommen, dass der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird.	
	OE.1	Das Einsatzgebiet des Kartenterminals ist eindeutig definiert.
AE.2	Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen.	
	OE.2	bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt.
AE.3	Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheitstechnische Veränderungen am Kartenterminal vorgenommen wurden.	
	OE.3	bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt.
AE.4	Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet.	
	OE.4	bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt.
AE.5	Es wird angenommen, dass der Benutzer während der PIN-Eingabe über das PIN-Pad den Status der LED beziehungsweise des LCD-Displays dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.	
	OE.5	bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt.

8.2 Erklärung der Sicherheitsanforderungen

Der TOE entspricht zusammen mit den Anforderungen an die Umgebung den sicherheitstechnischen Anforderungen.
Auch ein Angreifer mit hohem Angriffspotential kann die Sicherheitsfunktionen, Speicherwiederaufbereitung und Schutz der PIN nicht manipulieren, da der Speicher definiert aufbereitet wird und der Austausch der PIN nur zwischen Chipkarte und TOE über die Kartenleserschnittstelle erfolgt. Diese befindet sich im TOE und wird gegen Manipulation mit Sicherheitssiegel geschützt.
Somit ist der TOE konsistent mit den Sicherheitszielen.

Die Sicherheitsziele des TOE sehen vor, die Identifikationsdaten nicht zu speichern und/oder preiszugeben. Sicherheitstechnische Veränderungen müssen erkennbar sein.
Die Widerstandfähigkeit des TOE gegen Angreifer mit hohem Angriffspotential spiegelt sich in den über EAL3 hinausgehenden Anforderungen

- ADO_DEL.2
- ADV_IMP.1
- ADV_LLD.1
- ALC_TAT.1
- AVA_MSU.3
- AVA_VLA.4

wieder.

8.2.1 Zusammenhänge: Sicherheitsziele – Sicherheitsanforderungen

Tabelle 13: Sicherheitsziele – Sicherheitsanforderungen

Sicherheitsziele	Sicherheits-anforderungen	Kommentar
O.1	FDP_RIP.2	Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos beziehungsweise dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED beziehungsweise das sichere Zeichen zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.
O.2	FTA_TAB.1	Während sich der TOE im sicheren PIN-Eingabemodus befindet, wird dieser Zustand durch eine rotblinkende LED beziehungsweise durch das Aufleuchten des sicheren Zeichens im LCD-Display angezeigt.
O.3	FDP_ACC.1 FDP_ACF.1	Der TOE überträgt die PIN nur zur Chipkarte
O.4	FDP_ACC.1 FDP_ACF.1	Der TOE leitet nur PIN-Kommandos mit zulässigen Instructionsbytes an die Chipkarte weiter.
O.5	FPT_PHP.1	Der TOE stellt sicher, dass sicherheitstechnische Veränderungen am TOE durch das Sicherheitssiegel erkennbar sind.

8.2.2 Querverweise: Sicherheitsziele – Sicherheitsanforderungen

In der nachfolgenden Tabelle wird für jede identifizierte Sicherheitsanforderung aufgezeigt, zu welchen Sicherheitszielen sie beiträgt.

Tabelle 14: Sicherheitsziele – Sicherheitsanforderungen

	O.1	O.2	O.3	O.4	O.5
FDP_ACC.1			**X**	**X**	
FDP_ACF.1			**X**	**X**	
FDP_RIP.2	**X**				
FTA_TAB.1		**X**			
FPT_PHP.1					**X**

8.2.3 Abhängigkeiten der funktionalen Sicherheitsanforderungen

Tabelle 15 beinhaltet die Abhängigkeiten der funktionalen Sicherheitsanforderungen.

Tabelle 15: Abhängigkeiten

Sicherheits-anforderungen	Abhängigkeiten	Referenz
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 Nicht zutreffend
FDP_RIP.2	Keine	-
FTA_TAB.1	Keine	-
FPT_PHP.1	FMT_MOF.1	Nicht zutreffend

FDP_ACC.1

FDP_ACF.1

- Zugriffskontrolle basierend auf Sicherheitsattributen

FDP_ACF.1

FDP_ACC.1

- Teilweise Zugriffskontrolle

FMT_MSA.3

- Initialisierung statischer Attribute
- Keine Abhängigkeit für den TOE, da keine Veränderung der Sicherheitsattribute möglich ist, wodurch ein Management der Sicherheitsattribute entfallen kann. Die Identität der Subjekte und Objekte stellt schon an sich das Sicherheitsattribut dar. Dadurch ist die Initialisierung weiterer Sicherheitsattribute nicht notwendig.

FDP_RIP.2

Keine Abhängigkeiten

FTA_TAB.1

Keine Abhängigkeiten

FPT_PHP.1

FMT_MOF.1

- Management des Verhaltens der Sicherheitsfunktionen
- Keine Abhängigkeit für den TOE, da keine Veränderung des Verhaltens der Sicherheitsfunktion möglich ist, wodurch ein Management des Verhaltens der Sicherheitsfunktionen entfallen kann.

8.2.4 Zuordnung der Sicherheitsanforderungen an die IT-Umgebung

Es gibt keine Anforderungen an die IT-Umgebung.

8.3 Erklärung der TOE-Übersichtsspezifikation

8.3.1 Sicherheitsanforderungen und Sicherheitsfunktionen

Die in der folgendenden Tabelle zusammengefassten Sicherheitsfunktionen entsprechen und ergänzen die Sicherheitsanforderungen des TOE.
Alle Sicherheitsanforderungen werden durch die vorhandenen Sicherheitsfunktionen, die sich gegenseitig zu einem sicheren Gesamtsystem ergänzen, abgedeckt.

Tabelle 16: Sicherheitsfunktionen Sicherheitsanforderungen

	Sicherheits-funktion	**Sicherheits-anforderung**	**Kommentar**
SF.1	Speicherwieder-aufbereitung	FDP_RIP.2	Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos beziehungsweise dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED beziehungsweise das sichere Zeichen zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.
SF.2	Schutz der PIN	FDP_ACC.1 FDP_ACF.1	Das Umschalten des Kartenterminals in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach [CCID] durchgeführt. Dieses CT-Kommando enthält die PIN-Handlingsvereinbarungen und das Chipkartenkommando, in welches die PIN an die spezifizierte Stelle integriert wird. Anhand des Instructionbytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN-Kommando handelt (siehe Tabelle 17), welches explizit eine PIN-Eingabe erwartet. Im PIN-Eingabemodus wird die Eingabe der persönlichen Identifikationsdaten im RAM zwischengespeichert, um sie nach erfolgreicher Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden.
		FTA_TAB.1	Der PIN-Eingabemodus wird optisch durch ein rotes Blinken der SPE-LED beziehungsweise das Aufleuchten des sicheren Zeichens im Display angezeigt bis die Vollständigkeit der PIN erreicht, beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit. Der Eingabefortschritt wird mittels Übertragung von Dummycodes ~~[*]~~ dem System mitgeteilt. Be der Variante mit LCD-Display wird der Eingabefortschritt zusätzlich im Display mit ~~Dummycodes~~Sternchen [*] dargestellt.

Tabelle 17: Instructionbytes [ISO 7816]/[EMV 2000]

INS-Byte:	**Bezeichnung:**	**Bedeutung**	**Norm:**
20_h	VERIFY	PIN-Eingabe	ISO/IEC 7816-4
24_h	CHANGE REFERENCE DATA	PIN ändern	ISO/IEC 7816-8
26_h	DISABLE VERIFICATION REQUIREMENT	PIN aktivieren	ISO/IEC 7816-8
28_h	ENABLE VERIFICATION REQUIREMENT	PIN deaktivieren	ISO/IEC 7816-8
$2C_h$	RESET RETRY COUNTER	PIN entsperren	ISO/IEC 7816-8

Tabelle 18 Zuordnung: Sicherheitsanforderungen - Sicherheitsfunktionen

Sicherheitsanforderungen	SF.1	SF.2
FDP_ACC.1		**x**
FDP_ACF.1		**x**
FDP_RIP.2	**x**	
FTA_TAB.1		**x**

8.3.2 Sicherheitsanforderungen und Sicherheitsmaßnahmen

Tabelle 19: Sicherheitsmaßnahmen Sicherheitsanforderungen

	Sicherheits-maßnahmen	Sicherheits-anforderung	Kommentar
SM.1	Versiegelung	FPT_PHP.1	Die Anforderung der Sicherheit vor materieller Manipulation des TOE wird nicht durch eine Sicherheitsfunktion (SF) als Bestandteil der TSF erfüllt, sondern wird durch die Sicherheitsmaßnahme (SM) der Versiegelung gewährleistet.

8.3.3 Anforderungen und Maßnahmen zur Vertrauenswürdigkeit

Tabelle 20: Anforderungen und Maßnahmen zur Vertrauenswürdigkeit

	Maßnahme zur Vertrauenswürdigkeit	Anforderungen an die Vertrauens-würdigkeit	Kommentar
M.1	Konfigurations-management	ACM_CAP.3	Autorisierungskontrolle
		ACM_SCP.1	TOE – CM – Umfang
M.2	Auslieferung und Betrieb	**ADO_DEL.2**	**Erkennung von Modifizierungen**
		ADO_IGS.1	Installations-, Generierungs-, und Anlaufprozeduren
M.3	Informell funktionale Spezifikation	ADV_FSP.1	Informell funktionale Spezifikation
M.4	Sicherheitsspezifischer Entwurf auf hoher Ebene	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
M.5	**Darstellung der Implementierung**	**ADV_IMP.1**	**Teilmenge der Implementierung der TSF**
M.6	**Entwurf auf niedriger Ebene**	**ADV_LLD.1**	**Beschreibender Entwurf auf niedriger Ebene**
M.7	Informeller Nachweis der Übereinstimmung	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
M.8	Handbücher	AGD_ADM.1	Quick-Start Instructions und Betriebsdokumentation
		AGD_USR.1	
M.9	Lebenszyklus – Unterstützung	ALC_DVS.1	Identifikation der Sicherheitsmaßnahmen
		ALC_TAT.1	**Klar festgelegte Entwicklungswerkzeuge**
M.10	Test-Dokumentation	ATE_COV.2	Analyse der Testabdeckung
		ATE_DPT.1	Testen – Entwurf auf hoher Ebene
		ATE_FUN.1	Funktionales Testen
		ATE_IND.2	Unabhängiges Testen – Stichprobenartig
M.11	Schwachstellen-bewertung	**AVA_MSU.3**	**Analysieren und Testen auf unsichere Zustände**
		AVA_SOF.1	Stärke der TOE-Sicherheitsfunktionen
		AVA_VLA.4	**Hohe Widerstandsfähigkeit**

8.4 Erklärung der PP-Postulate

Es ist keine Konformität zu einem PP vorgesehen.

9. Anhang

9.1 Abkürzungen

APDU	Applikation Programming Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CardMan	Geschutztes Warenzeichen der OMNIKEY AG für Smart Card Reader
CC	Common Criteria, see [CC]
CT	Card Terminal
DIN	Deutsches Institut für Normung e.V.
EAL	Evaluation Assurance Level
EMV	Europay, Mastercard, Visa
EVG	Evaluierungsgegenstand (=TOE)
HBCI	Home Banking Computer Interface
IBM	International Business Machines
ICC	Integrated Chip Card
ISO	International Organization for Standardization
IT	Informationstechnik
M	Maßnahme
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PP	Protection Profile
RAM	Random Access Memory
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Gesetz zur digitalen Signatur
SigV	Verordnung zur digitalen Signatur
SOF	Strength Of Function
SPE	Secure PIN Entry
SF	Sicherheitsfunktion
SM	Sicherheitsmaßnahme
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TÜVIT	TÜV Informationstechnik
US	United States
USB	Universal Serial Bus

9.2 Literaturverzeichnis

[CC]	ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security —, First edition 1999-12-01 ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements ISO/IEC 15408-3:1999(E), Part 3: Security assurance requirements
[SigG]	Signaturgesetz [SigG], Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, vom 16.Mai.2001
[SigV]	Signaturverordnung [SigV] , Verordnung zur elektronischen Signatur, vom 16. November 2001
[CCID]	Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001
[ISO 7816]	DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands
[EMV 2000]	EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000
[PC/SC]	Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 1.0, Dezember 1997
[DIN NI-17.4]	DIN NI-17.4, Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Version 1.0, vom 30. November 1998
[BSI 7500]	BSI 7500 Druckschrift, Produkte für die materielle Sicherheit, Version 1.00, Kapitel .4 Sicherheitsetiketten