

# Common-Criteria-Dokument

## Sicherheitsvorgaben EAL3+

|                       |                  |                             |
|-----------------------|------------------|-----------------------------|
| <b>Project</b>        | <b>Name:</b>     | <b>KB SCR Pro</b>           |
|                       | <b>Firmware:</b> | <b>1.06</b>                 |
|                       |                  |                             |
| <b>Zertifizierung</b> | <b>BSI-ID:</b>   | <b>BSI-DSZ-CC-0405</b>      |
| <b>Bestätigung</b>    | <b>BSI-ID:</b>   | <b>BSI.02082.TE.xx.2006</b> |
| <b>Dokument</b>       | <b>Name:</b>     | <b>FSC_ASE_V130.doc</b>     |
|                       | <b>Version:</b>  | <b>1.30</b>                 |
|                       | <b>Status:</b>   | <b>Final</b>                |
|                       | <b>Date:</b>     | <b>13.09.2006</b>           |
|                       |                  |                             |
|                       | <b>Author:</b>   | <b>Marcus Hartmann</b>      |

---

Fujitsu Siemens Computers GmbH  
Bürgermeister Ulrich Straße 100  
D-86199 Augsburg

---

## Revision History

| Date       | Version | Description                         | Author          |
|------------|---------|-------------------------------------|-----------------|
| 08.11.2004 | 1.22    | Finale Version FW 104, zertifiziert | Marcus Hartmann |
| 13.09.2006 | 1.30    | Erweiterungen FW 106                | Marcus Hartmann |
|            |         |                                     |                 |
|            |         |                                     |                 |
|            |         |                                     |                 |
|            |         |                                     |                 |
|            |         |                                     |                 |
|            |         |                                     |                 |

© Copyright 2004-2006 – All rights reserved

The information, knowledge and presentations contained in this documentation are property of Fujitsu Siemens Computers GmbH. The documentation or information contained, knowledge and presentations must not be made accessible to others, published or distributed in any other way, neither completely nor partly, directly nor indirectly, without the permission in writing of Fujitsu Siemens Computers GmbH.

## Inhaltsverzeichnis

|   |           |
|---|-----------|
| <b>1. ST-Einführung „ASE_INT.1“</b> .....   | <b>5</b>  |
| <b>1.1 ST Identifikation</b> .....  | <b>5</b>  |
| <b>1.2 Erklärung der Sachnummern</b> .....  | <b>6</b>  |
| 1.2.1 Übersicht: Sachnummer – Firmware:.....                                      | 6         |
| <b>1.3 ST Übersicht</b> .....   | <b>6</b>  |
| <b>1.4 Postulat der Übereinstimmung mit den [CC]</b> .....                        | <b>7</b>  |
| <b>2. TOE-Beschreibung „ASE_DES.1“</b> .....                                      | <b>8</b>  |
| <b>3. TOE-Sicherheitsumgebung „ASE_ENV.1“</b> .....                               | <b>10</b> |
| <b>3.1 Annahmen</b> .....   | <b>10</b> |
| <b>3.2 Bedrohungen</b> .....  | <b>11</b> |
| <b>3.3 Organisatorische Sicherheitspolitik</b> .....                              | <b>11</b> |
| <b>4. Sicherheitsziele „ASE_OBJ.1“</b> .....                                      | <b>12</b> |
| <b>4.1 Sicherheitsziele für den TOE</b> .....                                     | <b>12</b> |
| <b>4.2 Sicherheitsziele für die Umgebung</b> .....                                | <b>12</b> |
| <b>4.3 Zusammenhänge: Anforderungen [SigG]/[SigV] - Sicherheitsziele</b> .....    | <b>13</b> |
| <b>5. IT-Sicherheitsanforderungen „ASE_REQ.1“</b> .....                           | <b>14</b> |
| <b>5.1 Funktionale Sicherheitsanforderungen an den TOE</b> .....                  | <b>14</b> |
| 5.1.1 Schutz der Benutzerdaten (Klasse FDP).....                                  | 15        |
| 5.1.2 TOE-Zugriff (Klasse FTA).....   | 17        |
| 5.1.3 Schutz der TSF (Klasse FPT).....  | 17        |
| <b>5.2 Anforderungen an die Mindeststärke der TOE-Sicherheitsfunktionen</b> ..... | <b>18</b> |
| <b>5.3 Anforderungen an die Vertrauenswürdigkeit des TOE</b> .....                | <b>18</b> |
| <b>5.4 Sicherheitsanforderungen an die IT-Umgebung</b> .....                      | <b>18</b> |
| <b>6. TOE-Übersichtsspezifikation „ASE_TSS.1“</b> .....                           | <b>19</b> |
| <b>6.1 TOE-Sicherheitsfunktionen</b> .....  | <b>19</b> |
| <b>6.2 TOE-Sicherheitsmaßnahme Versiegelung (SM.1)</b> .....                      | <b>20</b> |
| <b>6.3 Maßnahmen zur Vertrauenswürdigkeit</b> .....                               | <b>20</b> |
| <b>7. PP-Postulate „ASE_PPC.1“</b> .....  | <b>20</b> |
| <b>8. Erklärung</b> .....   | <b>21</b> |
| <b>8.1 Erklärung der Sicherheitsziele</b> .....                                   | <b>21</b> |
| 8.1.1 Abwehr der Bedrohungen durch den TOE .....                                  | 22        |
| 8.1.2 Berücksichtigung der Annahmen .....   | 23        |
| <b>8.2 Erklärung der Sicherheitsanforderungen</b> .....                           | <b>24</b> |
| 8.2.1 Zusammenhänge: Sicherheitsziele – Sicherheitsanforderungen .....            | 25        |
| 8.2.2 Querverweise: Sicherheitsziele – Sicherheitsanforderungen .....             | 25        |
| 8.2.3 Abhängigkeiten der funktionalen Sicherheitsanforderungen .....              | 26        |
| 8.2.4 Zuordnung der Sicherheitsanforderungen an die IT-Umgebung .....             | 26        |
| <b>8.3 Erklärung der TOE-Übersichtsspezifikation</b> .....                        | <b>27</b> |
| 8.3.1 Sicherheitsanforderungen und Sicherheitsfunktionen.....                     | 27        |
| 8.3.2 Sicherheitsanforderungen und Sicherheitsmaßnahmen .....                     | 28        |
| 8.3.3 Anforderungen und Maßnahmen zur Vertrauenswürdigkeit.....                   | 28        |
| <b>8.4 Erklärung der PP-Postulate</b> .....                                       | <b>28</b> |
| <b>9. Anhang</b> .....  | <b>29</b> |

|            |                                   |           |
|------------|-----------------------------------|-----------|
| <b>9.1</b> | <b>Abkürzungen .....</b>          | <b>29</b> |
| <b>9.2</b> | <b>Literaturverzeichnis .....</b> | <b>30</b> |

# 1. ST-Einführung „ASE\_INT.1“

## 1.1 ST Identifikation

Titel: Common-Criteria-Dokument  
Sicherheitsvorgaben EAL3+ für KB SCR Pro  
Version: 1.30  
Datum: 13.09.2006  
Datei Name: FSC\_ASE\_V130.doc  
Autor(en): Marcus Hartmann / Werner Waitz  
Zert. ID: **BSI-DSZ-CC-0405**  
Best. ID: **BSI.02082.TE.xx.2006**

Der Evaluationsgegenstand ist die Chipkartenleser-Tastatur KB SCR Pro (**TOE=Target of Evaluation**) mit der Firmware-Version **1.06** der Hersteller Fujitsu Siemens Computers GmbH und Omnikey GmbH. Die Sachnummer lautet: S26381-K329-V2\*\* HOS:01. Diese basiert auf einer frühere Evaluierung/Zertifizierung (Firmware 104 und 104\*).

### **Abbildung: KB SCR Pro**



USB Smartcard Reader Keyboard, side slot: 26381-K329-V2\*\* HOS:01

## 1.2 Erklärung der Sachnummern

Die Sachnummer ist in vier Blöcke aufgeteilt. *Beispiel: S26381-K329-V220 HOS:01*

Block1: „S26381“ Fujitsu Siemens Computers Sachnummernkreis für Tastaturen und Chipkartenleser

Block2: „K329“ Produktfamilie (Technologie, Gehäuseform, Schnittstelle)  
 K329 = USB-Chipkartenlesertastatur mit Kartenschlitz von rechts  
 K339 = USB-Chipkartenlesertastatur mit Kartenschlitz von oben

Block3: „V220“ Die Hunderterstelle hinter dem V kennzeichnet die Gehäusefarbe  
 1 = bright light grey  
 2 = bright light grey (neue Windows Taste)  
 3 = zukünftige Farbe 2  
 4 = anthrazit  
 5 = silber

Block3: „V220“ die Zehner- und Einerstelle der hinter V kennzeichnet die Tastaturbeschriftung

weitere Beispiele:  
 10 = US (United States)  
 11 = H (Hungary)  
 20 = D (German)  
 65 = GB (Great Britain)

Block4: „HOS:01“ kennzeichnet den Gerätestand (Versionsnummer) einer Tastatur  
 S26381-K329-V220 HOS:01 = Firmware 1.06

### 1.2.1 Übersicht: Sachnummer – Firmware:

| Tastaturvariante:    | Sachnummer:             | Firmware: |
|----------------------|-------------------------|-----------|
| Tastatur KBPC CX:    | S26381-K329-V1xx HOS:02 | 1.04      |
| Tastatur KBPC CX:    | S26381-K329-V1xx HOS:04 | 1.04*     |
| Tastatur KB SCR Pro: | S26381-K329-V2xx HOS:01 | 1.06      |

Die Sachnummern ist auf der Rückseite der Tastatur aufgebracht. Bei in Folie eingeschweißten Tastaturen kann man die Sachnummer direkt von der Rückseit ablesen. Auf diese Nummern wird im Handbuch hingewiesen.

## 1.3 ST Übersicht

Beim TOE handelt es sich um eine USB-Tastatur mit integriertem Chipkartenterminal 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 die gesamte Tastatur mit integriertem Kartenleser im Folgenden „Kartenterminal“ genannt. Neben der normalen Tastaturfunktionalität stellt der TOE mit Hilfe eines integrierten Kartenlesers die Möglichkeit zur Verfügung, kontaktbehaftete Speicher- und Prozessorchipkarten zu verarbeiten. 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:

- **Tastatur mit festem USB Kabel**
- **Handauflage**
- **Bedienungsanleitung (Sicherheitshinweise)**

Darüber hinaus wird der TOE kundenspezifisch mit weiteren Komponenten ausgeliefert, 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 den Nummernblock in den PIN-Eingabemodus umschaltet. Optisch wird dies dem Nutzer über die rot blinkende SPE-LED (LED4) angezeigt. Nach erfolgreicher Eingabe der PIN wird diese direkt zur Chipkarte gesendet und anschließend wieder in die Tastaturfunktion zurückgekehrt. Die PIN wird nur zur Chipkarte hin übertragen.

Das Kartenterminal bietet die Option die PIN nur über den Nummernblock (numerisch) oder zusätzlich über das alphanumerische Feld (alphanumerisch) einzugeben. Im Default-Zustand kann die PIN nur über den Nummernblock eingegeben werden. Das alphanumerische Feld hat in dieser Option keine Funktion.

Da das Keyboardlayout sprachabhängig ist und die Firmware keine Kenntnis über das jeweilige Keyboardlayout des einzelnen Kartenterminals besitzt, ist sie nicht in der Lage die Tastencodes ohne zusätzliche Information den ACSII-Codes zuzuweisen. Deshalb kann die Nutzung des alphanumerischen Feldes zur PIN-Eingabe nur durch die Übertragung einer sprachabhängigen Code-Tabelle erfolgen. Diese Code-Tabelle wird benutzt, um die Tastencodes in ASCII-Codes zu transformieren. Die Code-Tabelle wird vom Treiber in den Speicher des TOE geschrieben, sobald die Code-Tabelle an einer definierten Stelle in der Registrierung des Hostsystem eingetragen ist. Über ein Firmware-Flag wird die alphanumerische Option beim Herunterladen gesetzt und somit auch alphanumerische Zeichen zugelassen.

Durch die Wahlfreiheit der Code-Tabelle können allerdings auch falsche (ungewollte) Zuordnungen im alphanumerischen Tastenfeld entstehen, die letztlich auch zur Sperrung einer Chipkarte führen können. Aber auch nach der Übertragung der Code-Tabelle ist die Eingabe der PIN über den Nummernblock sicher, da der Nummernblock von der Code-Tabelle nicht beeinflusst wird.



Der Eingabefortschritt wird bei beiden Optionen mittels der Übertragung von Dummycodes [\*] dem System mitgeteilt. Bei beiden Optionen wird sichergestellt, daß die Sicherheitsfunktionen des TOE immer aktiv sind, gleichgültig ob eine Code-Tabelle geladen wurde oder nicht. Somit werden Eingaben im sicheren Modus (bei rot blinkender LED) 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 sichere PIN-Eingabe**

| <b>Funktion</b>    | <b>Nummernblock</b> | <b>alphanumerisches Feld</b> |
|--------------------|---------------------|------------------------------|
| Eingabebestätigung | [Enter]             | [↵]                          |
| Abbruch            | [+]                 | [ESC]                        |
| Backspace          | [-]                 | [←]                          |

Die PIN wird nur zur Chipkarte übertragen bzw. 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, werden am Produkt über die Trennkante zwischen Gehäuseober- und Unterteil authentische und fälschungssichere Siegel aufgebracht, welche gewährleisten, 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.

Tastatur und Kartenterminal werden 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 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 bzw. herstellereklärte Signaturanwendungsprogramme 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 als Kartenterminal 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 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 über den Nummernblock den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.  |
| AE.6     | Es wird angenommen, daß der Benutzer die PIN über den Nummernblock eingibt.  |

### 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 als Kartenterminal 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 (Siegelnummer) 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 über den Nummernblock der Tastatur muß der Benutzer den Status der LEDs dahingehend überprüfen, daß der Modus der sicheren PIN-Eingabe aktiv ist. |
| OE.6                              | Der Benutzer muß die PIN über den Nummernblock eingeben.  |

### 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   | Sicherheitsziel  | Beschreibung   |
|--------------------------|--|--|--|
| §15 Abs. 4 [SigV]        | Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar sein  | O.5<br><br>OE.3  | Sicherheitstechnische Veränderungen am TOE müssen durch das Sicherheitssiegel erkennbar sein.<br><br>Der Anwender muß das Sicherheitssiegel (Siegelnummer) 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<br><br>O.2<br><br>O.3<br><br>O.4<br><br>OE.5<br><br>OE.6 | Die PIN wird außer zum Zeitpunkt der Verarbeitung vom TOE nicht gespeichert.<br><br>Der TOE stellt sicher, daß dem Anwender die sichere PIN-Eingabe eindeutig signalisiert wird.<br><br>Der TOE stellt sicher, daß die PIN nur zur Chipkarte übertragen wird.<br><br>Der TOE stellt sicher, daß die PIN nur über PIN-Kommandos mit zulässigen Instructionsbytes an die Chipkarte weitergeleitet wird.<br><br>Während der PIN-Eingabe über den Nummernblock der Tastatur muß der Benutzer den Status der LEDs dahingehend überprüfen, daß der Modus der sicheren PIN-Eingabe aktiv ist.<br><br>Der Benutzer muß die PIN über den Nummernblock eingeben. |

## 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 die Ausführung der Operationen Auswahl und Zuweisung durch kursive Schrift im Text der Komponenten gekennzeichnet.

**Tabelle 7: Funktionale Anforderungen an den TOE**

| Nr. | ID         | Klasse / Komponente   | Abhängigkeiten         |
|-----|------------|---|------------------------|
|     | <b>FDP</b> | <b>Schutz der Benutzerdaten</b>                             |                        |
| 1   | FDP_ACC.1  | Teilweise Zugriffskontrolle                                 | FDP_ACF.1              |
| 2   | FDP_ACF.1  | Zugriffskontrolle basierend auf Sicherheitsattributen       | FDP_ACC.1<br>FMT_MSA.3 |
| 3   | FDP_RIP.2  | Vollständiger Schutz bei erhalten gebliebenen Informationen | Keine                  |
|     |            |   |                        |
|     | <b>FTA</b> | <b>TOE-Zugriff</b>  |                        |
| 4   | FTA_TAB.1  | TOE-Zugriffswarnmeldung                                     | Keine                  |
|     |            |   |                        |
|     | <b>FPT</b> | <b>Schutz der TSF</b>                                       |                        |
| 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 Tastaturschnittstelle*
- *PC über USB-Schnittstelle*
- *Chipkarte über Kartenleserschnittstelle*

die Objekte:

- *PIN*
- *LED zur Anzeige der sicheren PIN-Eingabe*

und die durch die *Chipkartenleser-Zugriffspolitik* abgedeckten Operationen:

- *PIN-Eingabe*
- *Übermittlung der PIN*
- *Ansteuerung der LED*

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 Tastaturschnittstelle*
- *PC über USB-Schnittstelle*
- *Chipkarte über Kartenleserschnittstelle*

*Die Objekte sind:*

- *PIN*
- *LED zur Anzeige der sicheren PIN-Eingabe*

*Die Operationen sind:*

- *PIN-Eingabe*
- *Übermittlung der PIN*
- *Ansteuerung der LED*

##### 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 (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<sub>h</sub>*
- *CHANGE REFERENCE DATA (ISO/IEC 7816-8) INS=24<sub>h</sub>*
- *DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=26<sub>h</sub>*
- *ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=28<sub>h</sub>*
- *RESET RETRY COUNTER (ISO/IEC 7816-8) INS=2C<sub>h</sub>*

*Die PIN (Objekt) kann vom Benutzer (Subjekt) über den Nummernblock der Tastatur 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 bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED zur Anzeige der sicheren PIN-Eingabe ausgeschaltet. Die Speicheraufbereitung stellt sicher, daß keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal nach Abschluß der PIN-Eingabe oder Entnahme der Karte vorhanden sind.*

*Das Ausschalten der LED 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 im sicheren Eingabemodus befindet, wird dieser Zustand durch eine rotblinkende LED angezeigt, die 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

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 Angriffspotential 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+)**

| Vertrauenswürdigkeitsklasse        | Vertrauenswürdigkeitsfamilie | 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                        |
| Konfigurationsmanagement           | ACM_CAP.3                    | Autorisierungskontrolle                              |
|                                    | ACM_SCP.1                    | TOE – CM – Umfang                                    |
| Auslieferung und Betrieb           | <b>ADO_DEL.2</b>             | <b>Erkennung von Modifizierungen</b>                 |
|                                    | ADO_IGS.1                    | Installations-, Generierungs-, und Anlaufprozeduren  |
| Entwicklung                        | ADV_FSP.1                    | Informell funktionale Spezifikation                  |
|                                    | ADV_HLD.2                    | Sicherheitsspezifischer Entwurf auf hoher Ebene      |
|                                    | <b>ADV_IMP.1</b>             | <b>Teilmenge der Implementierung der TSF</b>         |
|                                    | <b>ADV_LLD.1</b>             | <b>Beschreibender Entwurf auf niedriger Ebene</b>    |
|                                    | ADV_RCR.1                    | Informeller Nachweis der Übereinstimmung             |
| Handbücher                         | AGD_ADM.1                    | Systemverwalterhandbuch                              |
|                                    | AGD_USR.1                    | Benutzerhandbuch                                     |
| Lebenszyklus – Unterstützung       | ALC_DVS.1                    | Identifikation der Sicherheitsmaßnahmen              |
|                                    | <b>ALC_TAT.1</b>             | <b>Klar festgelegte Entwicklungswerkzeuge</b>        |
| 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               |
| Schwachstellenbewertung            | <b>AVA_MSU.3</b>             | <b>Analysieren und Testen auf unsichere Zustände</b> |
|                                    | AVA_SOF.1                    | Stärke der TOE-Sicherheitsfunktionen                 |
|                                    | <b>AVA_VLA.4</b>             | <b>Hohe Widerstandsfähigkeit</b>                     |

## 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-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 bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, daß keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal erhalten bleiben. Außerdem wird die LED 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 Nummernblocks im Kartenterminal 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 <sub>h</sub> | VERIFY                           | PIN-Eingabe      | ISO/IEC 7816-4 |
| 24 <sub>h</sub> | CHANGE REFERENCE DATA            | PIN ändern       | ISO/IEC 7816-8 |
| 26 <sub>h</sub> | DISABLE VERIFICATION REQUIREMENT | PIN aktivieren   | ISO/IEC 7816-8 |
| 28 <sub>h</sub> | ENABLE VERIFICATION REQUIREMENT  | PIN deaktivieren | ISO/IEC 7816-8 |
| 2C <sub>h</sub> | RESET RETRY COUNTER              | PIN entsperren   | ISO/IEC 7816-8 |

Durch Umschalten des Nummernblocks 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 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.

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 Sicherheitssiegeln, 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 (Zerstöreeigenschaften) 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 | OE.6 |
|------|-----|-----|-----|-----|-----|------|------|------|------|------|------|
| 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    |      |
| AE.6 |     |     |     |     |     |      |      |      |      |      | 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.5, da der Anwender das Sicherheitssiegel regelmäßig vor der Benutzung des Gerätes 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.                         |
| 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 angezeigt wird  |
|      | OE.5  | Unterstützt zusätzlich die Abwehr der Bedrohung T.2, da der Anwender die Anzeige (LED) 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 der Benutzung des Gerätes 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 der Benutzung des Gerätes 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 Sicherheits Siegels 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.1, da der Anwender das Sicherheitsiegel regelmäßig vor der Benutzung des Gerätes 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.   |

### 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 der Tastatur 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 und regelmäßig vor Benutzung des Gerätes 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 den Nummernblock den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.   |   |
|      | OE.5   | bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt. |
| AE.6 | Es wird angenommen, dass der Benutzer die PIN über den Nummernblock eingibt.   |   |
|      | OE.6   | 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 | Sicherheitsanforderungen | Kommentar  |
|------------------|--------------------------|--|
| O.1              | FDP_RIP.2                | Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED 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 angezeigt.   |
| O.3              | FDP_ACC.1<br>FDP_ACF.1   | Der TOE überträgt die PIN nur zur Chipkarte  |
| O.4              | FDP_ACC.1<br>FDP_ACF.1   | Der TOE leitet nur PIN-Kommandos mit zulässigen Instructionsbytes an die Chipkarte weiter.   |
| O.5              | FTP_PHP.1                | Der TOE stellt sicher, dass sicherheitstechnische Veränderungen am TOE durch das Sicherheitsiegel 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      |
|------------------|----------|----------|----------|----------|----------|
| <b>FDP_ACC.1</b> |          |          | <b>X</b> | <b>X</b> |          |
| <b>FDP_ACF.1</b> |          |          | <b>X</b> | <b>X</b> |          |
| <b>FDP_RIP.2</b> | <b>X</b> |          |          |          |          |
| <b>FTA_TAB.1</b> |          | <b>X</b> |          |          |          |
| <b>FTP_PHP.1</b> |          |          |          |          | <b>X</b> |

### 8.2.3 Abhängigkeiten der funktionalen Sicherheitsanforderungen

Tabelle 15 beinhaltet die Abhängigkeiten der funktionalen Sicherheitsanforderungen.

**Tabelle 15: Abhängigkeiten**

| Sicherheitsanforderungen | Abhängigkeiten         | Referenz                      |
|--------------------------|------------------------|-------------------------------|
| FDP_ACC.1                | FDP_ACF.1              | FDP_ACF.1                     |
| FDP_ACF.1                | FDP_ACC.1<br>FMT_MSA.3 | FDP_ACC.1<br>Nicht zutreffend |
| FDP_RIP.2                | Keine                  | -                             |
| FTA_TAB.1                | Keine                  | -                             |
| FTP_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

#### FTP\_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 folgenden 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**

|      | Sicherheitsfunktion        | Sicherheitsanforderung                  | Kommentar  |
|------|----------------------------|---|--|
| SF.1 | Speicherwiederaufbereitung | FDP_RIP.2                               | Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.   |
| SF.2 | Schutz der PIN             | FDP_ACC.1<br>FDP_ACF.1<br><br>FTA_TAB.1 | Das Umschalten des Nummernblocks im Kartenterminal 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.<br><br>Der PIN-Eingabemodus wird optisch durch ein rotes Blinken der SPE-LED 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. |

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

| INS-Byte:       | Bezeichnung:                     | Bedeutung        | Norm:          |
|-----------------|----------------------------------|------------------|----------------|
| 20 <sub>h</sub> | VERIFY                           | PIN-Eingabe      | ISO/IEC 7816-4 |
| 24 <sub>h</sub> | CHANGE REFERENCE DATA            | PIN ändern       | ISO/IEC 7816-8 |
| 26 <sub>h</sub> | DISABLE VERIFICATION REQUIREMENT | PIN aktivieren   | ISO/IEC 7816-8 |
| 28 <sub>h</sub> | ENABLE VERIFICATION REQUIREMENT  | PIN deaktivieren | ISO/IEC 7816-8 |
| 2C <sub>h</sub> | 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

|      | Sicherheitsmaßnahmen | Sicherheitsanforderung | Kommentar   |
|------|----------------------|------------------------|---|
| SM.1 | Versiegelung         | FTP_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 Vertrauenswürdigkeit         | Kommentar  |
|-------------|---|---|--|
| M.1         | Konfigurationsmanagement                        | ACM_CAP.3<br>ACM_SCP.1                            | Autorisierungskontrolle<br>TOE – CM – Umfang   |
| M.2         | Auslieferung und Betrieb                        | <b>ADO_DEL.2</b><br>ADO_IGS.1                     | <b>Erkennung von Modifizierungen</b><br>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  |
| <b>M.5</b>  | <b>Darstellung der Implementierung</b>          | <b>ADV_IMP.1</b>                                  | <b>Teilmenge der Implementierung der TSF</b>   |
| <b>M.6</b>  | <b>Entwurf auf niedriger Ebene</b>              | <b>ADV_LLD.1</b>                                  | <b>Beschreibender Entwurf auf niedriger Ebene</b>  |
| M.7         | Informeller Nachweis der Übereinstimmung        | ADV_RCR.1   | Informeller Nachweis der Übereinstimmung   |
| M.8         | Handbücher                                      | AGD_ADM.1<br>AGD_USR.1                            | Quick-Start Instructions und Betriebsdokumentation   |
| M.9         | Lebenszyklus – Unterstützung                    | ALC_DVS.1<br><b>ALC_TAT.1</b>                     | Identifikation der Sicherheitsmaßnahmen<br><b>Klar festgelegte Entwicklungswerkzeuge</b>   |
| M.10        | Test-Dokumentation                              | ATE_COV.2<br>ATE_DPT.1<br>ATE_FUN.1<br>ATE_IND.2  | Analyse der Testabdeckung<br>Testen – Entwurf auf hoher Ebene<br>Funktionales Testen<br>Unabhängiges Testen – Stichprobenartig   |
| <b>M.11</b> | <b>Schwachstellenbewertung</b>                  | <b>AVA_MSU.3</b><br>AVA_SOF.1<br><b>AVA_VLA.4</b> | <b>Analysieren und Testen auf unsichere Zustände</b><br>Stärke der TOE-Sicherheitsfunktionen<br><b>Hohe Widerstandsfähigkeit</b> |

## 8.4 Erklärung der PP-Postulate

Es ist keine Konformität zu einem PP vorgesehen.

## 9. Anhang

### 9.1 Abkürzungen

|       |   |
|-------|---|
| AP    | Advanced Performance                                |
| APDU  | Applikation Programming Data Unit                   |
| BSI   | Bundesamt für Sicherheit in der Informationstechnik |
| CC    | Common Criteria, see [CC]                           |
| CCKS  | Competence Center Keyboard Security                 |
| 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                     |
| HOS   | Haupt Objekt Stand                                  |
| IBM   | International Business Machines                     |
| ICC   | Integrated Chip Card                                |
| ISO   | International Organization for Standardization      |
| IT    | Informationstechnik                                 |
| NTK   | New Technology Keyboard                             |
| PC    | Personal Computer                                   |
| PC/SC | Personal Computer/Smart Card                        |
| PIN   | Personal Identification Number                      |
| PP    | Protection Profile                                  |
| RAM   | Random Access Memory                                |
| SigG  | Gesetz zur digitalen Signatur                       |
| SigV  | Verordnung zur digitalen Signatur                   |
| SOF   | Strength Of Function                                |
| 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                                |
| M     | Maßnahme  |

## 9.2 Literaturverzeichnis

|               |  |
|---------------|--|
| [CC]          | ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security —, First edition 1999-12-01<br>ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model<br>ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements<br>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<br>DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts<br>DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols<br>DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange<br>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   |