

Common-Criteria-Dokument

Sicherheitsvorgaben EAL3+

| | | |
|-----------------------|-------------------------|--|
| Project | Name: | Rezertifizierung SmartTerminal ST-2xxx |
| | ID: | 11772 |
| Zertifizierung | ID: | BSI-DSZ-CC-0660 |
| Bestätigung | ID: | BSI.02124.TE.07.2010 |
| Document | ID: | ST-2000_Rezert_Sicherheitsvorgaben- 20100223-V110.doc |
| | Version: | 1.10 |
| | Status: | Freigegeben |
| | Date: | 23.02.2010 |
| | Prepared by: | Jürgen Meier |
| | Date/Signature: | 02.12.2009 |
| | Checked by: | Robert Speckner |
| | Date/Signature: | 03.12.2009 |
| | Approved by: | Jürgen Meier |
| | Date/Signature : | 23.02.2010 |

Historie

| Datum | Version | Beschreibung | Autor |
|------------|---------|--|--------------|
| 21.09.2009 | 0.01 | Erstellung | Jürgen Meier |
| 30.09.2009 | 0.02 | Korrektur | Jürgen Meier |
| 19.10.2009 | 1.00 | Finale Überarbeitung | Jürgen Meier |
| 02.12.2009 | 1.10 | Gemäß OR_ST_091130_V1 überarbeitet Versionierung der Hardware mit aufgenommen | Jürgen Meier |
| 23.02.2010 | 1.10 | ST Identifikation um die Marke "Cherry" ergänzt | Jürgen Meier |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Verteilerliste

| Name | Firma/Abteilung | Beschreibung |
|----------------------------|----------------------------|------------------|
| Hans-Werner Blissenbach | TÜVIT in Essen | Evaluierung |
| Ragnar Kastenmaier | TÜVIT in Essen | Evaluierung |
| Robert Speckner | ZF Electronics GmbH / QP-C | Quality Planning |

© Copyright -2009 – All rights reserved

The information, knowledge and presentations contained in this documentation are property of ZF Electronics 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 ZF Electronics GmbH.

Inhaltsverzeichnis


| | | |
|-----------|--|-----------|
| 1. | ST-Einführung „ASE_INT.1“ | 4 |
| 1.1 | ST Identifikation | 4 |
| 1.2 | ST Übersicht | 6 |
| 1.3 | Postulat der Übereinstimmung mit den [CC] | 6 |
| 2. | TOE-Beschreibung „ASE_DES.1“ | 7 |
| 3. | TOE-Sicherheitsumgebung „ASE_ENV.1“ | 10 |
| 3.1 | Annahmen | 10 |
| 3.2 | Schutzbedürftige Werte | 11 |
| 3.3 | Bedrohungen | 11 |
| 3.4 | Organisatorische Sicherheitspolitik | 12 |
| 4. | Sicherheitsziele „ASE_OBJ.1“ | 12 |
| 4.1 | Sicherheitsziele für den TOE | 12 |
| 4.2 | Sicherheitsziele für die Umgebung | 13 |
| 4.3 | Zusammenhänge: Anforderungen [SigG]/[SigV] – Sicherheitsziele | 13 |
| 5. | IT-Sicherheitsanforderungen „ASE_REQ.1“ | 15 |
| 5.1 | Funktionale Sicherheitsanforderungen an den TOE | 15 |
| 5.1.1 | Schutz der Benutzerdaten (Klasse FDP) | 16 |
| 5.1.2 | TOE-Zugriff (Klasse FTA) | 18 |
| 5.1.3 | Schutz der TSF (Klasse FPT) | 18 |
| 5.1.4 | Kryptographische Unterstützung (Klasse FCS) | 19 |
| 5.2 | Anforderungen an die Mindeststärke der TOE-Sicherheitsfunktionen | 19 |
| 5.3 | Anforderungen an die Vertrauenswürdigkeit des TOE | 20 |
| 5.4 | Sicherheitsanforderungen an die IT-Umgebung | 20 |
| 6. | TOE-Übersichtsspezifikation „ASE_TSS.1“ | 21 |
| 6.1 | TOE-Sicherheitsfunktionen | 21 |
| 6.2 | TOE-Sicherheitsmaßnahme Versiegelung (SM.1) | 22 |
| 6.3 | Maßnahmen zur Vertrauenswürdigkeit | 23 |
| 7. | PP-Postulate „ASE_PPC.1“ | 23 |
| 8. | Erklärung | 23 |
| 8.1 | Erklärung der Sicherheitsziele | 24 |
| 8.1.1 | Abwehr der Bedrohungen durch den TOE | 25 |
| 8.1.2 | Berücksichtigung der Annahmen | 27 |
| 8.2 | Erklärung der Sicherheitsanforderungen | 28 |
| 8.2.1 | Zusammenhänge: Sicherheitsziele – Sicherheitsanforderungen | 29 |
| 8.2.2 | Querverweise: Sicherheitsziele – Sicherheitsanforderungen | 29 |
| 8.2.3 | Abhängigkeiten der funktionalen Sicherheitsanforderungen | 30 |
| 8.2.4 | Zuordnung der Sicherheitsanforderungen an die IT-Umgebung | 31 |
| 8.3 | Erklärung der TOE-Übersichtsspezifikation | 32 |
| 8.3.1 | Sicherheitsanforderungen und Sicherheitsfunktionen | 32 |
| 8.3.2 | Sicherheitsanforderungen und Sicherheitsmaßnahmen | 33 |
| 8.3.3 | Anforderungen und Maßnahmen zur Vertrauenswürdigkeit | 33 |
| 8.4 | Erklärung der PP-Postulate | 34 |
| 9. | Anhang | 35 |
| 9.1 | Abkürzungen | 35 |
| 9.2 | Literaturverzeichnis | 36 |

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

1. ST-Einführung „ASE_INT.1“

1.1 ST Identifikation

Titel: Common-Criteria-Dokument
 Sicherheitsvorgaben EAL3+ für das SmartTerminal ST-2xxx
 Dokumentversion: 1.10
 Datum: 23.02.2010
 Dok.- ID: Rezertifizierung SmartTerminal ST-2xxx
 Dateiname: ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc
 Autor(en): Jürgen Meier
 Zert.- ID: BSI-DSZ-CC-0660
 Bestätigungs- ID: BSI.02124.TE.07.2010

Der Evaluationsgegenstand ist ein Cherry Chipkartenterminal der Familie SmartTerminal ST-2xxx (**TOE = Target of Evaluation**) mit der Firmware-Version 6.01 und der Hardwareversion 03 der Hersteller ZF Electronics GmbH und SCM Microsystems GmbH. Die Vermarktung des Gerätes erfolgt unter der Marke **CHERRY** 

Die Rezertifizierung des TOE mit der Zertifizierungs- ID BSI-DSZ-CC-0660 basiert auf dem Rezertifizierungsverfahren BSI-DSZ-CC-0477 für die Produktversion SmartTerminal ST-2xxx mit der Firmware Version 5.11.

Der Evaluationsgegenstand unterteilt sich in folgende Produktvarianten:

- ST-2xxx xx Z –x

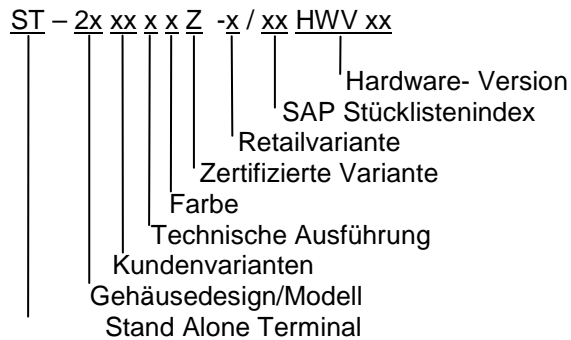
In allen Produktvarianten ist die gleiche zu evaluierende Firmware enthalten.

SCM Microsystems GmbH ist Entwickler und Hersteller der bestückten Leiterplatte des Chipkartenterminals ST-2xxx der Firma ZF Electronics GmbH. Treibersoftware und Firmware stammen ebenfalls aus dem Hause SCM.

SCM verwendet für die interne Bezeichnung des Produktes den Namen „SPR330“, der auf der Nomenklatur für SCM Produkte beruht. Daher wird z.B. in den Entwicklungsdokumentationen ADV, die sowohl für die SCM Produkte SPR532/SPR332/SPR132 als auch für die ZF Electronics GmbH Variante ST-2xxx gelten, dieser Bezeichner genutzt. In den öffentlichen Dokumenten wird nur die ZF Electronics Bezeichnung ST-2xxx verwendet.

| | | |
|------------|--|---------------|
| | ©ZF Electronics GmbH, 2009 | |
| 23.02.2010 | ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc | Seite 4 of 36 |

Nummernschlüssel: (Artikelnummer)



Hardware- Version:

Versionsverwaltung der Hardware 00 - 99

SAP Stücklistenindex:

Versionsnummer von 00 – 99 entsprechend der SAP Stückliste (siehe Spalte Vs)

Retailvariante:

R wenn als Retailvariante ausgeführt; ansonsten kein Kennzeichen

Zertifizierte Variante:

Z wenn als zertifizierte und bestätigte Variante ausgeführt; ansonsten entfällt Kennzeichen

Farbe :

Buchstaben von A - Z

C Gehäuseoberteil: grau Gehäuseunterteil: Druckguß blau chromatiert

Technische Ausführung:

Buchstaben von A - Z

U USB - Stecker

Kundenvarianten:

Nummer von 00 – 99

00 Standard

Gehäusedesign/Modell:

20 Chipkartenleser mit 16er Tastenfeld

1.2 ST Übersicht

Beim TOE handelt es sich um ein universelles Chipkartenlesegerät mit Keypad, welches die Funktionalität zur sicheren PIN-Eingabe sowie zum authentischen Firmware-Download bietet.

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.

1.3 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 2.3 August 2005) EAL3 mit Zusatz (ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4.

Die Stärke der Sicherheitsfunktion ist als SOF hoch klassifiziert.

2. TOE-Beschreibung „ASE_DES.1“

Der Chipkartenleser ST-2xxx stellt ein universelles Chipkartenlesegerät dar, das Prozessorchipkarten nach ISO7816 und EMV 2004 über verschiedene Applikationsschnittstellen (CT-API [1], PC/SC [3]) verarbeiten kann. Die Geräte arbeiten mit allen Chipkarten-Datenübertragungsprotokollen gemäß ISO 7816 [4] (T=0, T=1). Datenübertragungsprotokolle für Speicherchipkarten (I²C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt.

Der Chipkartenleser verfügt über ein Keypad mit Silikontasten, um eine sichere PIN-Eingabe zu garantieren. Er besitzt die numerischen Tasten „0“ bis „9“ sowie die Tasten „Clear“ (gelb), „Bestätigung“ (grün) und „Abbruch“ (rot). Des Weiteren sind drei Tasten „*“, „#“ und „F“ für zukünftige Funktionalitäten vorgesehen.

Der Leser erkennt die von der Host-Software übermittelten Kommandos zur PIN- Eingabe und fügt die über das Keypad eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Dabei wird nur die Tatsache an den Host gemeldet, dass eine der numerischen Tasten gedrückt wurde. Dies dient der Host-Applikation dem Anwender zu visualisieren, dass er eine Taste gedrückt hat bzw. wie viele Nummern der PIN aktuell eingegeben sind. Die PIN selbst verlässt den Leser nie in Richtung Host.

Die Leser können an allen Hostsystemen verwendet werden, die eine USB Schnittstelle besitzen. Sie werden als Zubehör im PC-Umfeld eingesetzt. Die Stromversorgung erfolgt über den USB- Bus.

Auf der Hostseite werden die Applikationsschnittstellen CT-API und PC/SC zur Verfügung gestellt, die für alle Chipkartenarten genutzt werden können. Alle Funktionalitäten an den Schnittstellen werden für CT-API gemäß [1] und für PC/SC gemäß [3] abgebildet. Weitere Schnittstellen (wie OCF) sind in Planung befindlich.

Der Chipkartenleser ST-2xxx besitzt keine Funktionalität, die ohne Anschluss an einen Host arbeitet. Er muss generell an einem Host betrieben werden.

Die Treiber der Chipkartenleser unterstützt folgende Betriebssysteme:

- Windows 98SE
- Windows ME
- Windows 2000
- Windows 2003 Server
- Windows XP
- Windows VISTA
- Windows CE (ab 5.0)
- Windows 7
- Linux
- MacOS X

Die Treibersoftware gehört nicht zum Evaluationsumfang. Der TOE endet an der USB Schnittstelle zum Host-Rechner.

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.

Die Chipkartenleser ST-2xxx sind wegen ihrer Multifunktionalität in vielen Marktsegmenten einsetzbar. Da die Chipkartenleser als Klasse 2 Leser [5] auch in der Lage sind, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (Signatur-Chipkarten) nach §2 Nummer 10 SigG auf sicherem Weg zu übermitteln, können sie auch für Applikationen gemäß Signaturgesetz und Signaturverordnung ([6], [7]) eingesetzt werden. Sie dienen des Weiteren zur Übermittlung des Hash-Wertes von der Anwendung zur Signaturkarte und zur Rückübertragung der Signatur von der Karte zur Signaturanwendung.

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

Sie stellen somit eine Teilkomponente für Signaturanwendungskomponenten dar, die eine Sicherheitsbestätigung benötigen, um für qualifizierte elektronische Signaturen nach §2 Nummer 3 SigG eingesetzt werden zu können.

Zur Verwendung des TOE gemäß SigG/SigV sind sowohl Applikationen (Signaturanwendungen) als auch Chipkarten, die im SigG- Kontext evaluiert und bestätigt wurden, einzusetzen.

Die Chipkartenleser ST-2xxx erfüllen die speziellen Anforderungen nach §15 Absatz 2 Nr.1a (keine Preisgabe oder Speicherung der Identifikationsdaten) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

Nachfolgende Liste der zur sicheren PIN- Eingabe unterstützten Instruction- Bytes sind von den Applikationen zu verwenden und von den Chipkarten spezifikationsgemäß zu unterstützen bzw. bei Nicht-Unterstützung mit einer geeigneten Fehlermeldung abzulehnen:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C
- UNBLOCK APPLICATION (EMV2004): INS=0x18

Die Chipkartenleser ST-2xxx bieten die Möglichkeit eines gesicherten Firmware-Downloads, um für zukünftige Anforderungen vorbereitet zu sein. Es werden dann sowohl zertifizierte und bestätigte als auch nicht zertifizierte Firmwareversionen zum Download bereitgestellt. Zertifizierte und bestätigte Versionen werden explizit unter Angabe der Zertifizierungs- ID als solche gekennzeichnet.

Der Firmware-Upgrade kann dann auf zwei unterschiedliche Arten geschehen:

- Der Kunde erhält von ZF Electronics eine CD mit einem Setup Programm, das die neue Firmware und ein Tool zum Auslesen der Firmwareversion und Laden der neuen Firmware enthält sowie die Treiber und eine detaillierte Anleitung zur Vorgehensweise. Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenleser überprüft, bevor die Firmware in den Controller geladen werden kann.
- Der Kunde lädt das Setup Programm mit neuer Firmware, einem Tool zum Auslesen der Firmwareversion und Laden der Firmware, den Treibern und einer detaillierte Anleitung zur Vorgehensweise von der Cherry Homepage unter <http://support.cherry.de>. Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenleser überprüft, bevor die Firmware in den Controller geladen werden kann.

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA- Algorithmus und einer Bitlänge von 2048 garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser.

Die sichere Generierung und Verwaltung der für die Erzeugung der sicheren Signatur notwendigen Schlüssel werden durch die Hersteller SCM Microsystems GmbH und ZF Electronics GmbH gewährleistet.

Die Hersteller garantieren, dass jede neue Version des TOEs eine neue Versionsnummer erhält und damit eindeutig identifizierbar ist.

Im Lieferumfang des Installationspaketes ist ein Software-Tool enthalten, welches die zertifizierte und bestätigte Firmware Version des Chipkartenlesers ST-2xxx überprüft. Durch Ausführen des Software Tools „FWCheck.exe“ V 6.1 bekommt der Benutzer die Firmware-Version des angeschlossenen Kartenterminals ST-2xxx angezeigt, und kann so überprüfen, ob es sich um die zertifizierte und bestätigte Firmware-Version 6.01 handelt. Dieses Software-Tool gehört nicht zum TOE.

Das Gehäuse ist mittels eines fälschungssicheren Sicherheitsaufklebers versiegelt, welcher sich bei Entfernung zerstört und damit nur einmal verwendbar ist.

| | | |
|------------|--|---------------|
| | ©ZF Electronics GmbH, 2009 | |
| 23.02.2010 | ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc | Seite 8 of 36 |

Die Chipkartenleser demonstrieren verschiedene Betriebszustände mittels zweier LEDs wie folgt:

| | LED1 (grün) | LED2 (orange) |
|---|-----------------------|-------------------------------|
| Just after Power-on/Just after DFU operation | OFF | OFF |
| Reader powered | ON | OFF |
| Smart card powered | ON | OFF |
| Smart card communication | 500ms ON 500ms OFF | OFF |
| Secure PIN entry mode | ON | 500ms ON 500ms OFF |
| PIN entry successfully completed, Smart card powered | ON | ON |
| PIN entry successfully completed, Smart card communication | 500ms ON 500ms OFF | ON |
| Smart card communication Error | 100ms ON 100ms OFF | Previous state |
| Firmware upgrade running | OFF | ON |
| Firmware upgrade failed | OFF | 32 ms ON 32 ms OFF |
| In BootROM mode | ON | ON |



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 der 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 TOE 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 1: Annahmen

Annahmen bezüglich der physikalischen Gegebenheiten

| Annahmen | Beschreibung |
|----------|--|
| AE.1 | Es wird angenommen, dass der EVG als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird. |

Annahmen bezüglich der personellen Gegebenheiten

| Annahmen | Beschreibung |
|----------|---|
| AE.2 | Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme und regelmäßig vor Benutzung des Geräts durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheitstechnischen Veränderungen am Kartenterminal vorgenommen wurden. |
| AE.3 | Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet. |
| AE.4 | Es wird angenommen, dass der Benutzer während der PIN- Eingabe über das Keypad den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN- Eingabe aktiv ist. |
| AE.5 | Es wird angenommen, dass der Benutzer die PIN über das Keypad eingibt. |
| AE.6 | Es wird angenommen, dass der Benutzer mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor Benutzung des Geräts verifiziert, ob die Versionsnummer des EVGs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG sollten automatisch verifizieren, dass nur bestätigte Versionen des EVGs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen |
| AE.7 | Es wird angenommen, dass der Benutzer bei einem Firmware-Update darauf achtet, dass die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist. |

Annahmen bezüglich der Anschlussmöglichkeiten bzw. der Anbindungen zu anderen IT- Systemen oder Produkten

| Annahmen | Beschreibung |
|----------|---|
| AE.8 | Es wird angenommen, dass ausschließlich Prozessorchipkarten benutzt werden, die den Spezifikationen [ISO 7816] bzw. [EMV 2004] genügen. |

3.2 Schutzbedürftige Werte

Folgende Werte müssen vom EVG und seiner Umgebung geschützt werden.

| Schützenswerte Größen | Beschreibung |
|-----------------------|--|
| PIN | Der Benutzer gibt die PIN über den Nummernblock des EVG ein. Diese wird dann vom EVG zur Chipkarte geschickt. Der EVG muss die Vertraulichkeit der PIN sicherstellen. |
| TSF Daten | Im EVG sind TSF Daten gespeichert die notwendig für den sicheren Betrieb sind. |

3.3 Bedrohungen

Im Folgenden werden alle gegen die Werte gerichteten Bedrohungen, die einen speziellen Schutz innerhalb des TOE oder in dessen Umgebung erforderlich machen und für den sicheren Betrieb des TOE relevant sind betrachtet. Es werden die Urheber von Bedrohungen identifiziert und anhand von Angriffen und angegriffenen Werten beschrieben. Es wird davon ausgegangen, dass ein Angreifer sehr gute Kenntnisse in Elektronik und Software besitzen muss. Die Motivation des Angreifers ist die PIN des Benutzers auszuspähen. Dabei könnte der Angreifer folgende Schwachstellen des TOE ausnutzen: die Schnittstelle zwischen Leser und Chipkarte, das Keypad zur PIN-Eingabe, den Firmware-Download. Gelegenheit zum Angriff bietet sich, wenn der TOE vom Benutzer unbeobachtet ist oder der Benutzer unvorsichtig bei der PIN-Eingabe ist.

Tabelle 2: 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, durch Manipulation des Sicherheits Siegels sicherheitstechnische Veränderungen am TOE vorzunehmen. |
| T.6 | Ein Angreifer könnte versuchen, durch Manipulation beim Download eine modifizierte oder fremde Firmware in den Leser zu laden, die Funktionalitäten zum Ausspähen der PIN beinhalten können. |

3.4 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 3: 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 Instructionbytes an die Chipkarte weiterleitet wird. |
| O.5 | Der TOE stellt sicher, dass sicherheitstechnische Veränderungen am TOE durch das Sicherheitsiegel erkennbar sind. |
| O.6 | Der TOE stellt sicher, dass nur der Download einer neuen Firmware akzeptiert wird, wenn die Integrität und Authentizität der Firmware verifiziert wurde. |

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 4 definiert.

Tabelle 4: Sicherheitsziele für die Umgebung

| Sicherheitsziele für die Umgebung | Beschreibung |
|-----------------------------------|---|
| OE.1 | Der TOE muss als Kartenterminal für die nichtöffentliche Umgebung eingesetzt werden. |
| OE.2 | Der Anwender darf ausschließlich Prozessorkarten benutzen, die den Spezifikationen [ISO 7816] bzw. [EMV 2004] 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 das Keypad 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 das Keypad eingeben. |
| OE.7 | Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifiziert, ob die Versionsnummer des TOEs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG sollten automatisch verifizieren, dass nur bestätigte Versionen des TOEs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen |
| OE.8 | Der Anwender muss darauf achten, dass bei einem Firmware-Upgrade die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet 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 5: 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 | Sicherheitstechnische Veränderungen am TOE müssen durch das Sicherheitssiegel erkennbar sein. |
| | | O.6 | Der TOE stellt sicher, dass nur der Download einer neuen Firmware akzeptiert wird, wenn die Integrität und Authentizität der Firmware verifiziert wurde. |

| | | | |
|--------------------------------|--|------|--|
| | | OE.3 | Der Anwender muss das Sicherheitssiegel (Siegelnummer) regelmäßig vor Benutzung des Gerätes auf Unversehrtheit prüfen. |
| | | OE.7 | Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifiziert, ob die Versionsnummer des TOEs mit der bestätigten Version übereinstimmt. |
| | | OE.8 | Der Anwender muss darauf achten, dass bei einem Firmware-Upgrade die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist |
| §15 Abs. 2 Nr. 1a [SigV] | Signaturanwendungs- komponenten 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 | Die PIN wird außer zum Zeitpunkt der Verarbeitung vom TOE nicht gespeichert. |
| | | 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 Instructionbytes an die Chipkarte weiterleitet wird. |
| | | OE.5 | Während der PIN-Eingabe über das Keypad des Kartenterminals 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 das Keypad 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. Es wurden die Ausführung der Operationen Auswahl und Zuweisung durch kursive Schrift im Text der Komponenten gekennzeichnet.

Tabelle 6: 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 | Keine |
| | FCS | Kryptographische Unterstützung | |
| 6 | FSC.COP.1 | Kryptographischer Betrieb | FDP_ITC.1 FCS_CKM.4 FMT_MSA.2 |

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 Keypad-Schnittstelle
- PC über USB-Schnittstelle
- Chipkarte über Kartenleserschnittstelle

die Objekte:

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

und die durch die Chipkartenleser-Zugriffspolitik abgedeckten Operationen:

- PIN-Eingabe
- Übermittlung der PIN
- Ansteuerung der LED
- Download gültiger signierter Firmware

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 Keypad-Schnittstelle
- PC über USB-Schnittstelle
- Chipkarte über Kartenleserschnittstelle

Die Objekte sind:

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

Die Operationen sind:

- PIN-Eingabe
- Übermittlung der PIN
- Ansteuerung der LED
- Download gültiger signierter Firmware

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

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

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= 0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-8) INS=0x24
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=0x26
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=0x28
- RESET RETRY COUNTER (ISO/IEC 7816-8) INS=0x2C
- UNBLOCK APPLICATION (EMV2004) INS=0x18

Die PIN (Objekt) kann vom Benutzer (Subjekt) über das Keypad eingegeben (Operation) werden.

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

Der vom PC (Subjekt) initiierte Download einer neuen Firmware (Operation) darf nur akzeptiert werden, wenn die Integrität und Authentizität der Firmware (Objekt) anhand ihrer Signatur mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 2048 erfolgreich verifiziert wurde

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 vom Mode der sicheren PIN-Eingabe in den entsprechenden Mode umgeschaltet.

Die Speicheraufbereitung stellt sicher, dass keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal nach Abschluss der PIN-Eingabe oder Entnahme der Karte vorhanden sind.

Das Umschalten der LED zur Anzeige der sicheren PIN-Eingabe stellt einen Statusübergang innerhalb des TOE dar. Der TOE signalisiert dem Benutzer, dass er sich jetzt in dem Zustand der sicheren PIN-Eingabe befindet. Nur in diesem Zustand ist eine PIN-Eingabe möglich. Das missbräuchliche provozieren einer PIN-Eingabe ist dadurch erkennbar.

| | | |
|------------|--|----------------|
| | ©ZF Electronics GmbH, 2009 | |
| 23.02.2010 | ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc | Seite 17 of 36 |

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

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 orange-blinkende LED angezeigt, die nach Beendigung statisch orange leuchtet.

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 (Zerstöreeigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann.

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

5.1.4 Kryptographische Unterstützung (Klasse FCS)

5.1.4.1 Kryptographischer Betrieb (Familie FCS_COP)

FCS_COP.1 Kryptographischer Betrieb RSA

FCS_COP.1.1

Die TSF müssen einen sicheren Firmware-Download mittels Entschlüsselung und Verifikation signierter Daten gemäß eines spezifizierten kryptographischen Algorithmus nach RSA und kryptographischer Schlüssellängen von 2048 bit, die den folgenden Normen

PKCS #1 Ver. 1.5, Abschnitt 10.2 und ISO/IEC 14888-2:2008, Abschnitt 6. entsprechen, durchführen.

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 2048 in Verbindung mit SFR.FCS_COP.1_SHA garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser.

FCS_COP.1 Kryptographischer Betrieb SHA

FCS_COP.1.1

Die TSF müssen einen sicheren Firmware-Download mittels Entschlüsselung und Verifikation signierter Daten gemäß eines spezifizierten kryptographischen Algorithmus nach SHA-256 und kryptographischer Schlüssellängen, welche hierbei nicht relevant sind, die den folgenden

Normen FIPS180-2 bzw. ISO/IEC 10118-3 entsprechen, durchführen.

Die Verifikation einer Signatur der Firmware basierend auf einem 256 Bit Hashwert gemäß SHA-256 in Verbindung mit SFR.FCS_COP.1_RSA garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser.

5.2 Anforderungen an die Mindeststärke der TOE-Sicherheitsfunktionen

Für alle funktionalen Sicherheitsanforderungen und Sicherheitsfunktionen, für die eine Betrachtung der Stärke (SOF) in Frage kommt, wird die Stärke SOF-Hoch gefordert. Im Einzelnen gilt:

Die TOE-Sicherheitsfunktion nutzen zwei Mechanismen, die einen sicheren Firmwaredownload garantieren. Für die Authentisierung der Firmware wird ein asymmetrischer RSA-Algorithmus mit einer Bitlänge von 2048 verwendet. Für die Sicherung der Integrität der Firmware wird die Hashfunktion SHA-256 mit einer Länge von 256 Bit eingesetzt.

Diese Mechanismen erreichen die Mindeststärke SOF-Hoch, wie vom SigG gefordert.

| | | |
|------------|--|----------------|
| | ©ZF Electronics GmbH, 2009 | |
| 23.02.2010 | ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc | Seite 19 of 36 |

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 7 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 |
| Konfigurationsmanagement | 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 |
| Schwachstellenbewertung | 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-Anzeige). Die Realisierung der einzelnen Sicherheitsfunktionen wird im Folgenden beschrieben.

Security Function 1: Schutz der PIN (SF.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, welches explizit eine PIN-Eingabe erwartet. In der folgenden Tabelle sind die zugelassenen Instructionbytes aufgeführt.

Tabelle 8 : Instructionbytes [ISO 7816]/[EMV 2004]

| INS-Byte: | Bezeichnung: | Bedeutung | Norm: |
|-----------|----------------------------------|------------------------|----------------|
| 0x20 | VERIFY | PIN eingeben | ISO/IEC 7816-4 |
| 0x24 | CHANGE REFERENCE DATA | PIN ändern | ISO/IEC 7816-8 |
| 0x26 | DISABLE VERIFICATION REQUIREMENT | PIN aktivieren | ISO/IEC 7816-8 |
| 0x28 | ENABLE VERIFICATION REQUIREMENT | PIN deaktivieren | ISO/IEC 7816-8 |
| 0x2C | RESET RETRY COUNTER | PIN entsperren | ISO/IEC 7816-8 |
| 0x18 | UNBLOCK APPLICATION | Applikation entblocken | EMV2004 |

Die Eingabe der persönlichen Identifikationsdaten wird 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 oranges Blinken der PIN-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. Dem Benutzer wird der Fortschritt seiner Eingabe mit dem Dummycode [*] für jede eingegebene Ziffer angezeigt. Die Ausgabe der Dummycodes erfolgt über die USB-Schnittstelle, die dann von der entsprechenden PC-Anwendung angezeigt wird. Innerhalb des TOE wird aber mit der korrekten PIN gearbeitet.

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.

| | | |
|---|--------------------------|---------------------------|
| Rezertifizierung SmartTerminal ST-2xxx | Common-Criteria-Dokument | Version 1.10, Freigegeben |
|---|--------------------------|---------------------------|

Security Function 2: Speicherwiederaufbereitung (SF.2)

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, dem Ziehen der Chipkarte, einem Timeout bei der PIN- Eingabe oder dem Abbruch durch den Benutzer wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, dass keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal erhalten bleiben. Der Speicherbereich beinhaltet sowohl die PIN als auch die APDU. 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. Dies wäre nur durch Download einer manipulierten Firmware möglich, was aber nicht möglich ist (siehe SF.3).

Security Function 3: Sicherer Firmwaredownload (SF.3)

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 2048 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den Chipkartenleser.

Der Hash-Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-256 mit einer Länge von 256 Bit ermittelt.

Die Verifikation der Integrität und Authentizität erfolgt im TOE durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im TOE gespeichert.

Ein Angreifer mit hohem Angriffspotential kann diese Sicherheitsfunktion nicht umgehen, da er nicht in den Besitz des privaten Schlüssels gelangen kann und somit den TOE nicht manipulieren kann. Da die Wahrscheinlichkeit den Schlüssel zu erraten oder zu errechnen zu gering ist, erfüllt der sichere Firmwaredownload die Mindeststärke der Funktionen „hoch“.

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 (Zerstöreeigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Das eingesetzte Siegel ist fälschungssicher, weist Authentizitätsmerkmale auf.

| | | |
|------------|--|----------------|
| | ©ZF Electronics GmbH, 2009 | |
| 23.02.2010 | ST-2000_Rezert_Sicherheitsvorgaben-20100223-V110.doc | Seite 22 of 36 |

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 9: Annahmen/Bedrohungen vs. Sicherheitsziele

| | O.1 | O.2 | O.3 | O.4 | O.5 | O.6 | OE.1 | OE.2 | OE.3 | OE.4 | OE.5 | OE.6 | OE.7 | OE.8 |
|------|-----|-----|-----|-----|-----|-----|------|------|------|------|------|------|------|------|
| 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 | | | | | |
| T.6 | | | | | | X | | | | | | | X | X |
| AE.1 | | | | | | | X | | | | | | | |
| AE.2 | | | | | | | | | X | | | | | |
| AE.3 | | | | | | | | | | X | | | | |
| AE.4 | | | | | | | | | | | X | | | |
| AE.5 | | | | | | | | | | | | X | | |
| AE.6 | | | | | | | | | | | | | X | |
| AE.7 | | | | | | | | | | | | | | X |
| AE.8 | | | | | | | | 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 10 ist die Abwehr der einzelnen Bedrohungen durch den TOE aufgeführt.

Tabelle 10: 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 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. |
| 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 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 wird. |
| | 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 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 Instructionbytes 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 2004] 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 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.6 | Ein Angreifer könnte versuchen, durch Manipulation beim Download eine modifizierte oder fremde Firmware in den Leser zu laden, die Funktionalitäten zum Ausspähen der PIN beinhalten können. | |
| | O.6 | Der TOE stellt sicher, dass nur der Download einer neuen Firmware akzeptiert wird, wenn die Integrität und Authentizität der Firmware verifiziert wurde. |
| | OE.7 | Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifiziert, ob die Versionsnummer des TOEs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG verifizieren, dass nur bestätigte Versionen des TOEs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen |
| | OE.8 | Der Anwender muss darauf achten, dass bei einem Firmware-Upgrade die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist. |

8.1.2 Berücksichtigung der Annahmen

Tabelle 11: Berücksichtigung der Annahmen

| | | |
|-------------|---|--|
| AE.1 | Es wird angenommen, dass der EVG als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird. | |
| | OE.1 | Das Einsatzgebiet des Kartenterminals ist eindeutig definiert. |
| AE.2 | Es wird angenommen, dass sich der Nutzer regelmäßig vor der 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.3 | Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet. | |
| | OE.4 | bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt. |
| AE.4 | Es wird angenommen, dass der Benutzer während der PIN- Eingabe über das Keypad 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.5 | Es wird angenommen, dass der Benutzer die PIN über das Keypad eingibt. | |
| | OE.6 | bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt. |
| AE.6 | Es wird angenommen, dass der Benutzer mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifiziert, ob die Versionsnummer des EVGs mit der bestätigten Version übereinstimmt. | |
| | OE.7 | Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifiziert, ob die Versionsnummer des EVGs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG verifizieren, dass nur bestätigte Versionen des EVGs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen |
| AE.7 | Es wird angenommen, dass der Benutzer bei einem Firmware-Update darauf achtet, dass die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist. | |
| | OE.8 | Der Anwender muss darauf achten, dass bei einem Firmware-Update die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist. |
| AE.8 | Es wird angenommen, dass ausschließlich Prozessorkarten benutzt werden, die den Spezifikationen [ISO 7816] bzw. [EMV 2004] genügen | |
| | OE.2 | 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 (SF.2) und Schutz der PIN (SF.1) 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 werden gegen Manipulation mit Sicherheitsiegel geschützt.

Der sichere Firmware-Download (SF.3) entspricht den Anforderungen nach der Mindeststärke der Funktionen „hoch“. Die Mindeststärke der Funktion „hoch“ ist angemessen und konsistent mit den Sicherheitszielen des EVGs der Nichtpreisgabe und Nichtspeicherung von Identifikationsdaten und der Erkennbarkeit sicherheitstechnischer Veränderungen.

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.

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.

8.2.1 Zusammenhänge: Sicherheitsziele – Sicherheitsanforderungen

Tabelle 12: 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 der LED-Mode zur Anzeige der sicheren PIN-Eingabe umgeschaltet. |
| O.2 | FTA_TAB.1 | Während sich der TOE im sicheren PIN-Eingabemodus befindet, wird dieser Zustand durch eine blinkende orange LED 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 Instructionbytes an die Chipkarte weiter. |
| O.5 | FPT_PHP.1 | Der TOE stellt sicher, dass sicherheitstechnische Veränderungen am TOE durch das Sicherheitssiegel erkennbar sind. |
| O.6 | FDP_ACC.1 FDP_ACF.1 FCS_COP.1 | Die Verifikation einer Signatur der Firmware mit dem Hash-Algorithmus SHA-256 und dem asymmetrischen RSA-Algorithmus mit einer Bitlänge von 2048 garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser. |

8.2.2 Querverweise: Sicherheitsziele – Sicherheitsanforderungen

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

Tabelle 13: Sicherheitsziele – Sicherheitsanforderungen

| | O.1 | O.2 | O.3 | O.4 | O.5 | O.6 |
|------------------|-----|-----|-----|-----|-----|-----|
| FDP_ACC.1 | | | X | X | | X |
| FDP_ACF.1 | | | X | X | | X |
| FDP_RIP.2 | X | | | | | |
| FTA_TAB.1 | | X | | | | |
| FPT_PHP.1 | | | | | X | |
| FCS_COP.1 | | | | | | X |

8.2.3 Abhängigkeiten der funktionalen Sicherheitsanforderungen

Tabelle 14 beinhaltet die Abhängigkeiten der funktionalen Sicherheitsanforderungen.

Tabelle 14: Abhängigkeiten

| Sicherheitsanforderungen | 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 | - |
| FTP_PHP.1 | Keine | Nicht zutreffend |
| FCS_COP.1 | <i>FDP_ITC.1</i> <i>FCS_CKM.4</i> <i>FMT_MSA.2</i> | Nicht zutreffend Nicht zutreffend 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

Keine Abhängigkeiten

FCS_COP.1 RSA

FDP_ITC.1

- *Import von Benutzerdaten ohne Sicherheitsattribute*
- Keine unmittelbare Abhängigkeit für den TOE, da der Schlüssel beim Hersteller eingebracht und mit dem TOE ausgeliefert wird

FCS_CKM.4

- *Zerstörung des kryptographischen Schlüssels*
- Ist eine Anforderung für die IT-Umgebung die Zerstörung des generierten privaten Schlüssel beschreibend
- Keine unmittelbare Abhängigkeit für den TOE, da dieser nur den öffentlichen Schlüssel enthält

FMT_MSA.2

- *Sichere Sicherheitsattribute*
- Keine Abhängigkeit für den TOE, da nur ein Schlüssel für den sicheren Firmware-Download vorhanden ist, wodurch ein Management der Sicherheitsattribute entfallen kann

FCS_COP.1 SHA

FDP_ITC.1

- *Import von Benutzerdaten ohne Sicherheitsattribute*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

FCS_CKM.4

- *Zerstörung des kryptographischen Schlüssels*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

FMT_MSA.2

- *Sichere Sicherheitsattribute*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

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 15: Sicherheitsfunktionen Sicherheitsanforderungen

| | Sicherheitsfunktion | Sicherheitsanforderung | Kommentar |
|------|-----------------------------------|---|--|
| SF.1 | Schutz der PIN | FDP_ACC.1 FDP_ACF.1 FTA_TAB.1 | Das Einschalten des 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 16), 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. Der PIN-Eingabemodus wird optisch durch ein Blinken der orangen PIN-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. |
| SF.2 | Speicherwieder- aufbereitung | 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 der LED-Mode zur Anzeige der sicheren PIN-Eingabe umgeschaltet. |
| SF.3 | Sicherer Firmware- download | FDP_ACC.1 FDP_ACF.1 FCS_COP.1 | Die Verifikation einer Signatur der Firmware mit dem Hash-Algorithmus SHA-256 und dem asymmetrischen RSA-Algorithmus mit einer Bitlänge von 2048 garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser. |

Tabelle 16: Instructionbytes [ISO 7816]/[EMV 2004]

| 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 |
| 18 _h | UNBLOCK APPLICATION | Applikation entblocken | EMV2004 |

Tabelle 17 Zuordnung: Sicherheitsanforderungen - Sicherheitsfunktionen

| Sicherheitsanforderungen | SF.1 | SF.2 | SF.3 |
|--------------------------|------|------|------|
| FDP_ACC.1 | x | | x |
| FDP_ACF.1 | x | | x |
| FDP_RIP.2 | | x | |
| FTA_TAB.1 | x | | |
| FCS_COP.1 | | | x |

8.3.2 Sicherheitsanforderungen und Sicherheitsmaßnahmen

Tabelle 18: 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 19: Anforderungen und Maßnahmen zur Vertrauenswürdigkeit

| | Maßnahme zur Vertrauenswürdigkeit | Anforderungen an die Vertrauenswürdigkeit | Kommentar |
|-------------|---|---|--|
| M.1 | Konfigurationsmanagement | 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 | Schwachstellenbewertung | 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

AP Advanced Performance
 APDU Applikation Programming Data Unit
 BSI Bundesamt für Sicherheit in der Informationstechnik
 CC Common Criteria, see [CC]
 CT Card Terminal
 DIN Deutsches Institut für Normung e.V.
 EAL Evaluation Assurance Level
 EMV Europay, Mastercard, Visa

HBCI Home Banking Computer Interface
 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

Zertifizierte Firmware – Firmware Version, mit der das Produkt nach Common Criteria EAL 3+ bestätigt wurde.

9.2 Literaturverzeichnis

| | |
|-----------------|--|
| [CC] | ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security —, Second edition 2005-10-01 ISO/IEC 15408-1:2005(E), Part 1: Introduction and general model ISO/IEC 15408-2:2005(E), Part 2: Security functional requirements ISO/IEC 15408-3:2005(E), Part 3: Security assurance requirements |
| [SigG] | Signaturgesetz [SigG], Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - Sig) ¹⁾ vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179) |
| [SigV] | Signaturverordnung [SigV] , Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), vom 16. November 2001 (BGBl. 2001 Teil I Nr. 59, S. 3074–3084) zuletzt geändert durch Art. 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631) |
| [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 2004] | EMV 2004 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.1, Mai 2004 |
| [PC/SC] | Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 2.0, November 1999 |
| [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 |
| NIST | NIST: FIPS Publication 180-2: Sicherer Hashstandard Aug 2002 und Änderungsmitteilung 1, Februar 2004 |
| ISO/IEC 10118-3 | IT- Sicherheitsverfahren Hash- Funktionen, Teil 3: Dedizierte Hash- Funktionen, 3rd ed., 2004 |
| ISO/IEC 14888-2 | IT- Sicherheitsverfahren – Elektronische Signaturen mit Anhang Teil 2: Ganze Zahlenfaktorenzerlegung basierte Mechanismen, 2008 |
| PKCS #1 V1.5 | Public Key Cryptography Standard, RSA Encryption Standard, Version 1.5, November 1993 |