Common-Criteria 2.3-Dokument

Sicherheitsvorgaben EAL3+

Project	**Name:**	**SmartCase KB SCR eSIG / K529**
	ID:	**10538**
Zertifizierung	**ID:**	**BSI-DSZ-CC-0525**
Bestätigung	**ID:**	**BSI.02107.TE.02.2010**
Document	**ID:**	**ASE_Security_Target-K529-20090909-V116.doc**
	Version:	**1.16**
	Status:	**Freigegeben**
	Date:	**09.09.2009**
	Prepared by:	**Jürgen Meier**
	Date/Signature:	**05.05.2008**
	Checked by:	**Jörg Kühnl**
	Date/Signature:	**30.05.2008**
	Approved by:	**Jürgen Meier**
	Date/Signature :	**09.09.2009**

Fujitsu Technology Solutions GmbH
Bürgermeister- Ulrich- Straße 100
D-86199 Augsburg

Historie

Datum	Version	Beschreibung	Autor
07.03.2008	0.01	Erstellung	Jürgen Meier
05.05.2008	0.02	Überarbeitung	Jürgen Meier
02.06.2008	1.00	Freigegeben	Jürgen Meier
16.07.2008	1.10	Einarbeitung der TÜV Kommentare aus OR1 und Korrektur Kap. 2 (Firmware-Download)	Jürgen Meier
05.08.2008	1.11	Umbenennung der SF.3	Jürgen Meier
17.09.2008	1.12	SHA-224 durch SHA-256 ersetzt	Jürgen Meier
12.01.2009	1.13	Instructionbyte- Auflistung korrigiert	Jürgen Meier
03.02.2009	1.14	FW Version von 1.00 auf 1.20 geändert, Umfirmierung eingearbeitet	Jürgen Meier
26.05.2009	1.15	Kap. 8.3.1 Tab. 15 und Tab. 17 FDP_ACC.1 und FDP_ACF.1 wurde SF.3 zugeordnet FCS_COP.1 Standards aktualisiert 9.2 Literaturverweise aktualisiert	Jürgen Meier
09.09.2009	1.16	Treiberunterstützung von Windows 7 eingefügt	Jürgen Meier

Verteilerliste

Name	Firma/Abteilung	Beschreibung
Hans-Werner Blissenbach	TÜViT Essen	Evaluierung
Peter Herrmann	TÜViT Essen	Evaluierung
Torsten Maykranz	SCM Microsystems	Senior Consultant PC Security Products
Jörg Kühnl	Cherry GmbH / ECE-PS	Engineering POS and Security Products

Inhaltsverzeichnis

1. ST-Einführung „ASE_INT.1“

1.1 ST Identifikation

Titel:	Common-Criteria 2.3-Dokument
	Sicherheitsvorgaben EAL3+ für SmartCase™ KB SCR eSIG
Dokumentversion:	1.16
Datum:	09.09.2009
Dok. ID	SmartCase KB SCR eSIG / K529
Dateiname:	ASE_Security_Target-K529-20090909-V116.doc
Autor(en):	Jürgen Meier
Zert. ID:	BSI-DSZ-CC-0525
Bestätigungs- ID:	BSI.02107.TE.02.2010

Der Evaluationsgegenstand (EVG) ist das Chipkartenterminal der Familie SmartCase™ KB SCR eSIG mit der Firmware-Version 1.20 der Hersteller Cherry GmbH und SCM Microsystems GmbH.

Der Evaluationsgegenstand unterteilt sich in folgende Produktvarianten:

- S26381-K529-Vxxx HOS:01

In allen Produktvarianten ist die gleiche zu evaluierende Firmware enthalten.

SCM Microsystems GmbH ist Entwickler der Elektronik- Hardware und der Firmware für das Chipkartenterminal SmartCase™ KB SCR eSIG. Die Treibersoftware stammt ebenfalls aus dem Hause SCM. Hersteller des Chipkartenterminals ist die Firma Cherry GmbH.
Produkteigner und Inverkehrbringer ist die Firma Fujitsu Technology Solutions GmbH.

Erklärung der Sachnummern

Die Sachnummer ist in vier Blöcke aufgeteilt. ***Beispiel: S26381-K529-V120 HOS:01***

Block1: „S26381“ Fujitsu Sachnummernkreis für Tastaturen und Chipkartenleser

Block2: „K529“ Produktfamilie (Technologie, Gehäuseform, Schnittstelle)
Chipkartenlesertastatur K529 = zertifiziert
Chipkartenlesertastatur K528 = nicht zertifiziert

Block3: „V120“ Die Hunderterstelle hinter dem V kennzeichnet die Gehäusefarbe z.B. 1 = marble grey; 2 = schwarz.

Block3: „V120“ 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-K529-V120 HOS:01 = Gerätestand 1.00

Die Sachnummern ist auf der Rückseite der Tastatur aufgebracht. Auf diese Nummern wird im Handbuch hingewiesen.

1.2 ST Übersicht

Beim EVG handelt es sich um eine Tastatur mit einem Klasse 2- Chipkartenleser, welche die Funktionalität zur sicheren PIN- Eingabe sowie zum authentischen Firmware-Download bietet.
Die Sicherheitsvorgaben stellen die funktionalen sowie organisatorischen Sicherheitsanforderungen und -prozeduren an den EVG 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.

2. EVG- Beschreibung „ASE_DES.1“

Der EVG, dass Chipkartenterminal KB SCR eSIG (S26381-K529-Vxxx HOS:01), stellt eine Tastatur mit einem integrierten Klasse 2 Leser dar, das Prozessorchipkarten nach ISO7816 und EMV über verschiedene Applikationsschnittstellen ([CT-API], [PC/SC] u.a.) verarbeiten kann. Die Geräte arbeiten mit allen Chipkarten-Datenübertragungsprotokollen gemäß [ISO 7816] (T=0, T=1). Datenübertragungsprotokolle für Speicherchipkarten (I^2C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt.

Das Chipkartenterminal erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe und fügt die 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 das Chipkartenterminal nie in Klartext. Die PIN- Eingabe ist nur über den Nummernblock der Tastatur möglich. Während sich das Terminal im sicheren PIN- Eingabemodus befindet ist eine PIN- Eingabe über den alphanumerischen Bereich nicht möglich.
Der sichere PIN- Eingabemodus wird dem Benutzer durch eine rote LED signalisiert. Die LEDs zur Statusanzeige des Chipkartenterminals sind durch einen Lichtleiter an die Gehäuseoberfläche nach oben geführt.

In der nachfolgende Tabelle sind die Funktionen und Tasten aufgeführt mit der die PIN- Eingabe bearbeitet bzw. bestätigt werden kann.

Funktion	**Nummernblock**		**alphanumerisches Feld**
	Taste	**Sonderbeschr.**	
Eingabebestätigung	[Enter]	[OK]	[↵]
Abbruch	[+]	[ABBRUCH]	[ESC]
Rückgängig	[-]	[←]	[←]

Tabelle 1: Tastenbelegung

Das Chipkartenterminal kann an allen Hostsystemen verwendet werden, die eine USB Schnittstelle besitzen.
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 gemäß [CT-API] und [PC/SC] Spezifikation abgebildet.

Die Treiber des Chipkartenterminals unterstützten folgende Betriebssysteme:

- Windows 2000
- Windows 2003 Server
- Windows XP
- Windows XP 64
- Windows VISTA
- Windows VISTA 64
- Windows 7
- Linux Kernel

Die Treibersoftware gehört nicht zum Evaluationsumfang.
Das Chipkartenterminal KB SCR eSIG besitzt keine Funktionalität, die ohne Anschluss an einen Host arbeitet. Er muss generell an einem Host betrieben werden.

Zum Lieferumfang gehören:

- Tastatur mit festem USB- Kabel
- CD mit Treiber und Softwaretools (optional, auch über Internet verfügbar)
- Manual und Betriebsdokumentation gemäß CC (optional, auch über Internet verfügbar)

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

Da das Chipkartenterminal als Klasse 2 Leser auch in der Lage ist, 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. Es dient des weiteren zur Übermittlung des Hash-Wertes von der Anwendung zur Signaturkarte und zur Rückübertragung der Signatur von der Karte zur Signaturanwendung.
Es stellt 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 EVG gemäß SigG/SigV sind sowohl Applikationen (Signaturanwendungen) als auch Chipkarten, die im SigG- Kontext evaluiert und bestätigt wurden, einzusetzen.
Das Chipkartenterminal KB SCR eSIG erfüllt 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
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x28
- UNBLOCK APPLICATION (EMV 2000): INS=0x18
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C

Das Chipkartenterminal KB SCR eSIG bieten die Möglichkeit eines gesicherten Firmware-Upgrade, um für zukünftige Anforderungen vorbereitet zu sein. Es werden nur zertifizierte und bestätigte Firmwareversionen zum Upgrade bereitgestellt. Die bereitgestellten Firmwaredateien werden explizit unter Angabe der Zertifizierungs- ID als zertifiziert und bestätigt gekennzeichnet. Diese ID kann auf der Internetseite der Bundesnetzagentur unter dem Sachgebiet Telekommunikation, elektronische Signatur eingesehen werden.

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

- Der Kunde erhält von Fujitsu Technology Solutions GmbH 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 aktuellen Treiber. Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenterminal 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 und den aktuellen Treiber von der Fujitsu Technology Solutions GmbH Homepage unter http://support.fujitsu-siemens.com/com/support/downloads.html Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenterminal überprüft, bevor die Firmware in den Controller geladen werden kann.

Die Verifikation der Signatur einer Firmware mit dem asymmetrischen RSA- Algorithmus und einer Bitlänge von 2048 sowie dem Hash- Verfahren SHA-256 garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in das Chipkartenterminal.
Das Laden einer nicht zertifizierten Firmware wird somit verhindert.

Die sichere Generierung und Verwaltung der für die Erzeugung der sicheren Signatur notwendigen Schlüssel werden durch die Hersteller SCM Microsystems GmbH und Cherry GmbH gewährleistet.
Die Hersteller garantieren, dass jede neue Version des EVG 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 Chipkartenterminal KB SCR eSIG überprüft. Durch Ausführen des Software Tools „FWCheck_KBSCReSIG.exe“ V 1.0 bekommt der Benutzer die Firmware-Version des angeschlossenen Kartenterminals KB SCR eSIG angezeigt, und kann so überprüfen, ob es sich um die zertifizierte und bestätigte Firmware-Version 1.20 handelt.
Dieses Software-Tool ist nicht Teil des EVG.

Das Gehäuse wird mittels fälschungssicherer Sicherheitsaufklebers versiegelt, welche sich bei Entfernung zerstören.
Durch die Anordnung der Siegel und die Auslegung des EVG- Gehäuses ist ein unautorisiertes Öffnen ohne einem Brechen der Siegel nicht möglich.
Dem Benutzer ist es somit möglich, und er wird dazu auch angehalten, die Unversehrtheit des Terminal zu überprüfen.
Sicherheitsrelevante Bauteile oder Datenleitungen sind im Inneren des Gehäuses so angeordnet, das Zugriffe über vorhandene Öffnungen im Gehäuse wie z.B. dem Kartenschacht nicht möglich sind.

3. EVG-Sicherheitsumgebung „ASE_ENV.1“

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

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

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

Um diesen Bedrohungen entgegen zu wirken wurden entsprechende Mechanismen integriert:

- Die sichere PIN- Eingabe wird durch eine LED angezeigt
- Speicherbereiche werden definiert aufbereitet
- Der EVG darf die PIN nur zur Chipkarte übertragen
- Die PIN darf nur über zugelassene PIN- Kommandos an die Chipkarte weitergegeben werden
- Der EVG wird durch Siegel geschützt
- Der Endanwender wird über seine Verantwortung während der Nutzung des EVGs informiert

3.1 Annahmen

Der EVG 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. herstellererklärte 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.8 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 EVGs 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 den Nummernblock 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 den Nummernblock 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 2000] 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 EVG oder in dessen Umgebung erforderlich machen und für den sicheren Betrieb des EVG 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 EVG ausnutzen: die Schnittstelle zwischen Leser und Chipkarte, der Nummernblock zur PIN- Eingabe, den Firmware-Update. Gelegenheit zum Angriff bietet sich, wenn der EVG vom Benutzer unbeobachtet ist oder der Benutzer unvorsichtig bei der PIN- Eingabe ist.

Bedrohungen	Beschreibung
T.1	Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den EVG 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 EVG in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln.
T.3b	Ein Angreifer könnte versuchen, die im EVG 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 Sicherheitssiegels sicherheitstechnische Veränderungen am EVG 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.

Tabelle 2: Bedrohungen

3.4 Organisatorische Sicherheitspolitik

Es sind keine organisatorischen Sicherheitspolitiken vorgesehen.

4. Sicherheitsziele „ASE_OBJ.1“

In diesem Kapitel werden die Sicherheitsziele für den EVG 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 EVG definiert, während in Kapitel 4.2 die Sicherheitsziele für die Umgebung des EVG 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 EVG

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

Tabelle 3: Sicherheitsziele für den EVG

Sicherheitsziele für den EVG	Beschreibung
O.1	Der EVG stellt sicher, dass die PIN, außer zum Zeitpunkt der Verarbeitung, nicht gespeichert wird.
O.2	Der EVG stellt sicher, dass dem Anwender die sichere PIN- Eingabe eindeutig signalisiert wird.
O.3	Der EVG stellt sicher, dass die PIN nur zur Chipkarte übertragen wird.
O.4	Der EVG stellt sicher, dass die PIN nur über PIN- Kommandos mit zulässigen Instructionbytes an die Chipkarte weitergeleitet wird.
O.5	Der EVG stellt sicher, dass sicherheitstechnische Veränderungen am EVG durch das Sicherheitssiegel erkennbar sind.
O.6	Der EVG 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 EVGs 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 EVG muss als Kartenterminal für die nichtöffentliche 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 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.
OE.7	Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifizieren, 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
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.

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**	**Sicher-heitsziel**	**Beschreibung**
§15 Abs. 4 [SigV]	Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar sein	O.5	Sicherheitstechnische Veränderungen am EVG müssen durch das Sicherheitssiegel erkennbar sein.
		O.6	Der EVG stellt sicher, dass nur der Download einer neue Firmware akzeptiert wird, wenn die Integrität und Authentizität der Firmware verifiziert wurde.

Gesetz / Verordnung	Gesetzestext	Sicher-heitsziel	Beschreibung
		OE.3 OE.7 OE.8	Der Anwender muss das Sicherheitssiegel (Siegelnummer) regelmäßig vor Benutzung des Gerätes auf Unversehrtheit prüfen. 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. Der Anwender muss darauf achten, dass bei einem Firmware-Update 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 O.2 O.3 O.4 OE.5 OE.6	Die PIN wird außer zum Zeitpunkt der Verarbeitung vom EVG nicht gespeichert. Der EVG stellt sicher, dass dem Anwender die sichere PIN-Eingabe eindeutig signalisiert wird. Der EVG stellt sicher, dass die PIN nur zur Chipkarte übertragen wird. Der EVG stellt sicher, dass die PIN nur über PIN-Kommandos mit zulässigen Instructionbytes an die Chipkarte weiterleitet wird. Während der PIN-Eingabe über den Nummernblock des Kartenterminals muss der Benutzer den Status der LEDs dahingehend überprüfen, dass der Modus der sicheren PIN-Eingabe aktiv ist. Der Benutzer muss die PIN über den Nummernblock eingeben.

5. IT-Sicherheitsanforderungen „ASE_REQ.1“

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

5.1 Funktionale Sicherheitsanforderungen an den EVG

In der nachfolgenden Tabelle sind alle funktionalen Anforderungen an den EVG 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 EVG

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	**EVG-Zugriff**	
4	FTA_TAB.1	EVG-Zugriffswarnmeldung	Keine
	FPT	**Schutz der TSF**	
5	FPT_PHP.1	Passive Erkennung materieller Angriffe	Keine
	FCS	**Kryptographische Unterstützung**	
6	FCS.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 EVG den Zugriff auf seine Betriebsmittel und somit alle durch den EVG 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 Tastatur-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 EVG erreichbar sind und pro Schnittstelle jeweils ein Subjekt definiert ist, ist die Identität der Objekte als Sicherheitsattribut ausreichend.
Die Subjekte sind:

- *Benutzer über die Tastatur-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

Anzeige des sicheren Eingabemodus vom EVG angesteuert (Operation) und die eingegebene PIN (Objekt) vom EVG 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 (EMV 2000): INS=0x18*

Die PIN (Objekt) kann vom Benutzer (Subjekt) über den Nummernblock eingegeben (Operation) werden.

Der EVG 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 EVG dar. Der EVG 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.

5.1.2 EVG- Zugriff (Klasse FTA)

5.1.2.1 EVG- Zugriffswarnmeldung (Familie FTA_TAB)

FTA_TAB.1 Vorgegebene EVG- Zugriffswarnmeldung

FTA_TAB.1.1

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

Während sich der EVG im sicheren Eingabemodus befindet, wird dieser Zustand durch eine rot-blinkende LED angezeigt.

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.

5.1.4 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-Update mittels Entschlüsselung und Verifikation signierter Daten *gemäß eines spezifizierten kryptographischen Algorithmus* nach RSA *und kryptographischer Schlüssellängen* von 2048 bit, *die den folgenden* Normen
ISO/IEC 14888 -1 /-2 und PKCS #1, Version 1.5
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-Update 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 EVG-Sicherheitsfunktionen

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

Die EVG- Sicherheitsfunktion „ Sicherer Firmware- Update“ nutzt zwei kryptographische Mechanismen.
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.
Beide Mechanismen sind nicht Umfang der Evaluierung und werden bei einer Ermittlung der Stärke der EVG- Sicherheitsfunktionen (SOF) nicht betrachtet.

5.3 Anforderungen an die Vertrauenswürdigkeit des EVG

Der EVG 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 EVG gegen Angreifer mit hohem Angriffpotential wird mit hoch eingestuft. Alle Anforderungen der Evaluationsstufe EAL3+ sind in der folgenden Tabelle aufgelistet. Die zusätzlichen Anforderungen für die Einstufung mit Zusatz sind fettgedruckt. Die Punkte AVA_MSU.1 und AVA_VLA.1 werden durch AVA_MSU.3 und AVA_VLA.4 ersetzt.

Tabelle 7 Anforderungen an die Vertrauenswürdigkeit (ASE und EAL3+)

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

5.4 Sicherheitsanforderungen an die IT- Umgebung

Es gibt keine Sicherheitsanforderungen an die IT- Umgebung.

6. EVG- Übersichtsspezifikation „ASE_TSS.1“

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

6.1 EVG- 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 EVG 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.

Sicherheitsfunktion 1: Sichere PIN- Eingabe (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 2000]

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
0x18	UNBLOCK APPLICATION	Applikation entblocken	EMV 2000
0x2C	RESET RETRY COUNTER	PIN entsperren	ISO/IEC 7816-8

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 eine rot blinkende 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 EVG 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 EVG über die Kartenleserschnittstelle erfolgt. Diese befindet sich im EVG und wird gegen Manipulation mit Sicherheitssiegel geschützt.

Sicherheitsfunktion 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 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. 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 EVG zu manipulieren. Dies wäre nur durch Download einer manipulierten Firmware möglich, was aber nicht möglich ist (siehe SF.3).

Sicherheitsfunktion 3: Sicherer Firmware-Update (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 EVG durch Vergleich des ermittelten Hash- Wertes und des Hash- Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im EVG 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 EVG nicht manipulieren kann. Da die Wahrscheinlichkeit den Schlüssel zu erraten oder zu errechnen zu gering ist, erfüllt der sichere Firmware-Update die Mindeststärke der Funktionen „hoch".

6.2 EVG- Sicherheitsmaßnahme Versiegelung (SM.1)

Anhand drei authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden.
Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist.
Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann.
Eine 7-stellige fortlaufende Nummer auf dem Siegel erlaubt eine eindeutige Identifizierung.
Das eingesetzte Siegel erfüllt die Sicherheitsstufe 2 gemäß BSI 7586 (Anforderungen und Prüfbedingungen an Sicherheitsetiketten) und ist in der Produktliste BSI 7500 gelistet.

6.3 Maßnahmen zur Vertrauenswürdigkeit

Der EVG 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 EVG (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 EVG-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 EVG- Sicherheitsumgebung identifiziert wurden, zurückverfolgbar und geeignet sind diese abzudecken.

Der EVG 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 EVG 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 EVG

In Tabelle 10 ist die Abwehr der einzelnen Bedrohungen durch den EVG aufgeführt.

Tabelle 10: Bedrohungen durch den EVG

T.1	Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den EVG 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 EVG 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 EVG 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 EVG 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 EVG 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 EVG als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird.
T.3b	Ein Angreifer könnte versuchen, die im EVG zwischengespeicherte PIN auszulesen.	
	O.1	Unterstützt die Abwehr der Bedrohung T.3b, da die PIN außer zum Zeitpunkt der Verarbeitung vom EVG nicht gespeichert wird.
	O.5	Unterstützt zusätzlich das Sicherheitsziel O.1 bei der Abwehr der Bedrohung T.3b, indem sicherheitstechnische Veränderungen am EVG 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 EVG 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 2000] genügen, gewährleistet wird, dass die zulässigen Instructionbytes nicht zum Speichern auf der Chipkarte dienen.
T.5	Ein Angreifer könnte versuchen, durch Manipulation des Sicherheitssiegels sicherheitstechnische Veränderungen am EVG vorzunehmen.	
	O.5	Unterstützt die Abwehr der Bedrohung T.5, indem sicherheitstechnische Veränderungen am EVG 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 EVG 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 EVG 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 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
	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.

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 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.5	Es wird angenommen, dass der Benutzer die PIN über den Nummernblock 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 2000] genügen	
	OE.2	bildet eine Zielvorgabe, die unmittelbar die Annahme umsetzt.

8.2 Erklärung der Sicherheitsanforderungen

Der EVG 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 EVG über die Kartenleserschnittstelle erfolgt. Diese befindet sich im EVG und werden gegen Manipulation mit Sicherheitssiegel geschützt.
Der sichere Firmware-Update (SF.3) entspricht den Anforderungen nach der Mindeststärke der Funktionen „hoch“. Die Mindeststärke der Funktion „hoch“ ist angemessen und konsistent mit den Sicherheitszielen des EVG der Nichtpreisgabe und Nichtspeicherung von Identifikationsdaten und der Erkennbarkeit sicherheitstechnischer Veränderungen.

Somit ist der EVG konsistent mit den Sicherheitszielen.

Die Sicherheitsziele des EVG sehen vor, die Identifikationsdaten nicht zu speichern und/oder preiszugeben. Sicherheitstechnische Veränderungen müssen erkennbar sein.
Die Widerstandfähigkeit des EVG 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 EVG 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	Sicherheits-anforderungen	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 EVG im sicheren PIN-Eingabemodus befindet, wird dieser Zustand durch eine blinkende rote LED angezeigt.
O.3	FDP_ACC.1 FDP_ACF.1	Der EVG überträgt die PIN nur zur Chipkarte
O.4	FDP_ACC.1 FDP_ACF.1	Der EVG leitet nur PIN-Kommandos mit zulässigen Instructionbytes an die Chipkarte weiter.
O.5	FPT_PHP.1	Der EVG stellt sicher, dass sicherheitstechnische Veränderungen am EVG durch das Sicherheitssiegel erkennbar sind.
O.6	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

Sicherheits-anforderungen	Abhängigkeiten	Referenz
FDP_ACC.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 Nicht zutreffend
FDP_RIP.2	Keine	-
FTA_TAB.1	Keine	-
FPT_PHP.1	Keine	-
FCS_COP.1	*FDP_ITC.1* *FCS_CKM.4* *FMT_MSA.2*	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 EVG, da keine Veränderung der Sicherheitsattribute möglich ist, wodurch ein Management der Sicherheitsattribute entfallen kann. Die Identität der Subjekte und Objekte stellt schon an sich das Sicherheitsattribut dar. Dadurch ist die Initialisierung weiterer Sicherheitsattribute nicht notwendig.

FDP_RIP.2

Keine Abhängigkeiten

FTA_TAB.1

Keine Abhängigkeiten

FPT_PHP.1

Keine Abhängigkeiten

FCS_COP.1 RSA

FDP_ITC.1

- *Import von Benutzerdaten ohne Sicherheitsattribute*
- Keine unmittelbare Abhängigkeit für den EVG, da der Schlüssel beim Hersteller eingebracht und mit dem EVG 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 EVG, da dieser nur den öffentlichen Schlüssel enthält

FMT_MSA.2

- *Sichere Sicherheitsattribute*
- Keine Abhängigkeit für den EVG, da nur ein Schlüssel für den sicheren Firmware-Update 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 EVG-Übersichtsspezifikation

8.3.1 Sicherheitsanforderungen und Sicherheitsfunktionen

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

Tabelle 15: Sicherheitsfunktionen Sicherheitsanforderungen

	Sicherheits-funktion	Sicherheits-anforderung	Kommentar
SF.1	**Sichere PÍN-Eingabe**	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 roten 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-Update**	FDP_ACC.1 FDP_ACF.1 FCS_COP.1	Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash- Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Die Verwendung des Hash-Algorithmus SHA-256 und des asymmetrischen RSA-Algorithmus mit einer Bitlänge von 2048 bit garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser.

Tabelle 16: Instructionbytes [ISO 7816]/[EMV 2000]

INS-Byte:	Bezeichnung:	Bedeutung	Norm:
20_h	VERIFY	PIN-Eingabe	ISO/IEC 7816-4
24_h	CHANGE REFERENCE DATA	PIN ändern	ISO/IEC 7816-8
26_h	DISABLE VERIFICATION REQUIREMENT	PIN aktivieren	ISO/IEC 7816-8
28_h	ENABLE VERIFICATION REQUIREMENT	PIN deaktivieren	ISO/IEC 7816-8
$2C_h$	RESET RETRY COUNTER	PIN entsperren	ISO/IEC 7816-8
18h	UNBLOCK APPLICATION	Applikation entblocken	EMV2000

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

	Sicherheits-maßnahmen	Sicherheits-anforderung	Kommentar
SM.1	**Versiegelung**	FPT_PHP.1	Die Anforderung der Sicherheit vor materieller Manipulation des EVG 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 Vertrauens-würdigkeit	Kommentar
M.1	Konfigurations-management	ACM_CAP.3	Autorisierungskontrolle
		ACM_SCP.1	EVG – CM – Umfang
M.2	Auslieferung und Betrieb	**ADO_DEL.2**	**Erkennung von Modifizierungen**
		ADO_IGS.1	Installations-, Generierungs-, und Anlaufprozeduren
M.3	Informell funktionale Spezifikation	ADV_FSP.1	Informell funktionale Spezifikation
M.4	Sicherheitsspezifischer Entwurf auf hoher Ebene	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
M.5	**Darstellung der Implementierung**	**ADV_IMP.1**	**Teilmenge der Implementierung der TSF**
M.6	**Entwurf auf niedriger Ebene**	**ADV_LLD.1**	**Beschreibender Entwurf auf niedriger Ebene**
M.7	Informeller Nachweis der Übereinstimmung	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
M.8	Handbücher	AGD_ADM.1	Quick-Start Instructions und Betriebsdokumentation
		AGD_USR.1	
M.9	Lebenszyklus – Unterstützung	ALC_DVS.1	Identifikation der Sicherheitsmaßnahmen
		ALC_TAT.1	**Klar festgelegte Entwicklungswerkzeuge**
M.10	Test-Dokumentation	ATE_COV.2	Analyse der Testabdeckung
		ATE_DPT.1	Testen – Entwurf auf hoher Ebene
		ATE_FUN.1	Funktionales Testen
		ATE_IND.2	Unabhängiges Testen – Stichprobenartig
M.11	Schwachstellen-bewertung	**AVA_MSU.3**	**Analysieren und Testen auf unsichere Zustände**
		AVA_SOF.1	Stärke der EVG-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 International, 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
EVG	Evaluationsgegenstand
TSF	EVG 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

BSI 7500	BSI- Technische Leitlinie BSI–TL 03400; Produkte für materielle Sicherheit (BSI 7500), November 2007
BSI 7586	BSI- Technische Leitlinie BSI-TL 03415; Anforderungen und Prüfbedingungen für Sicherheitsetiketten (BSI 7586), Ver.: 1.0 September 2005
[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
[CCID]	Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001
[CT-API]	Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen CT-API Version 1.1.1 / Juni 2001
[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
[EMV 2000]	EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000
[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
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 14888-1	IT - Sicherheitsverfahren - Elektronische Signaturen mit Anhang Teil 1: Allgemein, 2008
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
[PC/SC]	Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 2.0, November 1999
[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)