Bundesamt
für Sicherheit in der
Informationstechnik

# Common Criteria Protection Profile

# USB-Datenträger

Common Criteria

BSI-PP-0025

Version 1.4, 27.03.06

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

# Inhaltsverzeichnis

# 1 PP-Einführung

## 1.1 PP-Identifikation

| | | |
|---|---|---|
| 1 | PP-Name: | Schutzprofil (Protection Profile) für USB-Datenträger<br>BSI-PP-0025 |
| 2 | PP-Version: | 1.4 |
| 3 | Datum: | 27.03.2006 |
| 4 | | |
| 5 | Sponsor: | Bundesamt für Sicherheit in der Informationstechnik, Bonn |
| | Antragsteller: | Fachhochschule Bonn-Rhein-Sieg, St. Augustin |
| 6 | Autor: | Thomas Gilles |
| 7 | EVG-Name: | USB-Datenträger |
| 8 | EAL-Stufe: | EAL2+ |
| 9 | Suchbegriffe: | USB-Datenträger, USB-Stick, USB-Speicher,<br>USB-Festplatte, USB-Key-Drive, USB-Flash-Drive |
| 10 | CC-Version: | 2.1[1]<br>Berücksichtigt wurden alle Final Interpretations, die bis zum 27.03.2006 veröffentlicht wurden, |

[1] Dieses Dokument berücksichtigt die neue deutsche Rechtschreibung und passt die den CC entnommenen Texte dementsprechend teilweise an.

## 1.2 PP-Übersicht

11 Dieses Schutzprofil betrachtet alle Massenspeicher, die an die USB-Schnittstelle angeschlossen werden können. Diese Geräte werden als USB-Datenträger bezeichnet.

12 Geht ein USB-Datenträger verloren, wird verlegt oder entwendet so darf daraus nicht resultieren, dass die vertraulichen Daten im Speicher an unberechtigte Personen fallen. Des Weiteren darf es unberechtigten Personen nicht möglich sein, vertrauliche Daten auf dem Datenträger zu löschen oder zu manipulieren. Dazu definiert dieses Schutzprofil einen Basissatz an Sicherheitsanforderungen zur Wahrung der Vertraulichkeit, der Daten bei logischen und physischen Angriffen. Auch die Wahrung der Integrität der Daten im Falle einer Störung wird in den Anforderungen definiert.

13 Ein wesentlicher Aspekt der anwenderfreundlichen IT-Sicherheit des USB-Datenträgers ist die vollständige Implementierung der Sicherheitsfunktionen im Datenträger selbst. Dadurch wird die Nutzung des PP-konformen USB-Datenträgers an vielen Wirtssystemen möglich, da an diese keine SW-Anforderungen gestellt werden.

14 Eine einmalige Authentisierung reicht aus, um eine Verbindung zu den vertraulichen Daten zu etablieren. Nach der Authentisierung erbringt der Datenträger seine Sicherheitsleistung transparent.

15 Das Schutzprofil geht nur soweit auf HW-Annahmen ein, wie diese zwingend notwendig sind. Dies ermöglicht ein breites Spektrum an technischen Lösungen.

16 Es bleibt dem Hersteller überlassen, Produkte die zu diesem Schutzprofil konform sind, um zusätzliche Sicherheitsfunktionen zur Erhöhung der Sicherheitsleistung zu erweitern. Einige Hinweise dazu werden in Form von Anwendungsbemerkungen im PP vorgestellt. Die Erweiterungen können in den Sicherheitsvorgaben (Security Target – ST) spezifiziert werden, welche die Basis für eine Zertifizierung eines konkreten Produktes darstellen.

## 1.3 PP-Organisation

17 Die wesentlichen Bestandteile des Schutzprofils (Protection Profile – PP) sind

- die EVG-Beschreibung,
- die EVG-Sicherheitsumgebung,
- die Sicherheitsziele,
- die IT-Sicherheitsanforderungen und
- die Erklärung.

18 Die EVG-Beschreibung (Abschnitt 2) liefert allgemeine Informationen über den Evaluationsgegenstand (EVG), wie etwa den beabsichtigten Gebrauch und die Darstellung der zu schützenden Werte. Sie ist die Voraussetzung

zum Verständnis der Sicherheitsanforderungen. Dabei ist zu beachten, dass sich ein PP in der Regel nicht auf eine spezielle Implementierung bezieht, sondern eine Klasse gleichartiger Produkte beschreibt.

19 Die EVG-Sicherheitsumgebung (Abschnitt 3) legt in den Annahmen die Sicherheitsauflagen an die Umgebung, in der der EVG eingesetzt werden soll, dar. Dieses Kapitel kann als Auflagenkatalog an den Betreiber des EVGs angesehen werden. In den Abschnitten Bedrohungen und organisatorische Sicherheitspolitiken werden die vom EVG abzuwehrenden Bedrohungen oder die relevanten Gesetze, deren Einhaltung der EVG zu erfüllen hat, aufgeführt.

20 Die Sicherheitsziele (Abschnitt 4) legen produktunabhängig dar, wie der EVG den genannten Bedrohungen begegnet und wie er den organisatorischen Sicherheitspolitiken Rechnung trägt. Auch wird für jede Annahme an die EVG-Nutzung das damit verfolgte Sicherheitsziel erläutert.

21 Die IT-Sicherheitsanforderungen (Abschnitt 5) stellen die funktionalen Sicherheitsanforderungen an den EVG und seine Umgebung dar und definieren die Anforderungen an die Vertrauenswürdigkeit. Die Notation der Anforderungen entspricht der in den Common Criteria vordefinierten semiformalen Sprache.

22 Die Erklärung (Abschnitt 6) weist nach, dass das Schutzprofil eine vollständige und zusammengehörige Menge von IT-Sicherheitsanforderungen ist und dass ein zum Schutzprofil konformer EVG die Sicherheitsziele vollständig erfüllt.

23 Ein den Common Criteria genügendes Schutzprofil erfüllt gewisse Anforderungen hinsichtlich Form, Notation und Aufbau. Ein Glossar mit Erläuterungen zu den wichtigsten Abkürzungen der CC findet sich in den Abschnitten 1.4 und 1.5.

24 Zum besseren Verständnis des Schutzprofils sind Anwendungsbemerkungen eingearbeitet. Diese beinhalten Informationen, die nicht der Evaluation des Schutzprofils unterliegen und nur kommentierenden Charakter haben. Des Weiteren enthalten die Anwendungsbemerkungen Hinweise zu möglichen Sicherheitsfunktionen, die über die Anforderungen dieses Schutzprofils hinaus die Sicherheitsleistung erhöhen könnten.

## 1.4 Abkürzungen

| | |
|---|---|
| CC | Common Criteria |
| EAL | Evaluation Assurance Level (Vertrauenswürdigkeitsstufe) |
| EVG | Evaluationsgegenstand (Target of Evaluation – TOE) |
| FSP | Functional Specifications (Funktionale Spezifikation) |
| FSUD | Funktionale Sicherheitspolitik USB-Datenträger |
| HLD | High Level Design (Entwurf auf hoher Ebene) |
| HW | Hardware |
| PP | Protection Profile (Schutzprofil) |
| SFP | funktionale Sicherheitspolitik |
| SOF | Strength of Function (Stärke der Funktionen) |
| ST | Security Target (Sicherheitsvorgaben) |
| SW | Software |
| TOE | Target of Evaluation (Evaluationsgegenstand – EVG) |
| TSF | TOE Security Function (EVG-Sicherheitsfunktionen) |
| USB | Universal Serial Bus |

## 1.5 Glossar

| | |
|---|---|
| Authentisierungsmerkmal | Erforderliches Merkmal zur Freigabe der geschützten Daten. Z.B. ein Passwort, eine Chipkarte oder ein biometrisches Merkmal. |
| Benutzer | Besitzt das Authentisierungsmerkmal zur Freigabe seiner geschützten Daten. |
| Datenspur | Daten wie z.B. Auslagerungs- oder Protokolldaten, die nach Trennung des EVGs auf dem Wirtssystem zurückbleiben und möglicherweise Rückschlüsse auf vertrauliche Daten im Speicher des EVGs ermöglichen. |
| Evaluationsgegenstand | Dieser, den CC entnommene Begriff (engl.: TOE – Target of Evaluation) bezeichnet das IT-Produkt, die IT-Komponente oder das IT-System, das auf Erfüllung aller Sicherheitsanforderungen zu evaluieren ist. In diesem Schutzprofil stellt der USB-Datenträger den EVG da. |
| Freigabe | Durch erfolgreiche Authentisierung ermöglichter Zugriff auf die Daten des geschützten Speichers. |

| | |
|---|---|
| Papierkorb-Funktion | Löscht der Benutzer eine Datei, so wird diese Datei vom Betriebssystem des Wirtssystems nicht gelöscht, sondern in einen zentralen Ordner auf der Festplatte verschoben. |
| Schadsoftware | Bösartige Software wie Viren, Würmer oder Trojaner die eine potenzielle Gefahr für die Vertraulichkeit und Integrität der zu schützenden Daten des EVGs darstellen. |
| Sicherheitsfunktionen | EVG-Sicherheitsfunktionen (TSF) ist der Teil des EVGs, der für die Durchsetzung der Sicherheitspolitik verantwortlich ist. |
| Speicher | Ist der Teil des EVGs der zur Speicherung digitaler Daten bzw. Informationen genutzt wird. Die Implementierung der Sicherheitsfunktionen kann in diesem Speicher liegen. |
| Sitzung | Zeitraum zwischen Freigabe des EVGs und Verbindungstrennung. |
| Universal Serial Bus (USB) | Ein Bussystem zur Verbindung eines Computers mit externen USB-Peripheriegeräten zum Austausch von Daten. |
| Wirtssystem | Ein Computer mit USB-Schnittstelle an die der EVG angeschlossen wird. Über das Computersystem erfolgt der Zugriff auf die Daten des EVGs durch den Benutzer. |
| Zugriff | Die Möglichkeit, Daten auf dem EVG zu lesen, zu schreiben oder zu modifizieren. |

# 2 EVG-Beschreibung

25 Dieses Kapitel enthält neben der Darstellung des Evaluationsgegenstandes (EVG) allgemeine Informationen über den EVG, wie etwa den beabsichtigten Gebrauch und die Darstellung der zu schützenden Werte.

## 2.1 Produkt-Typ

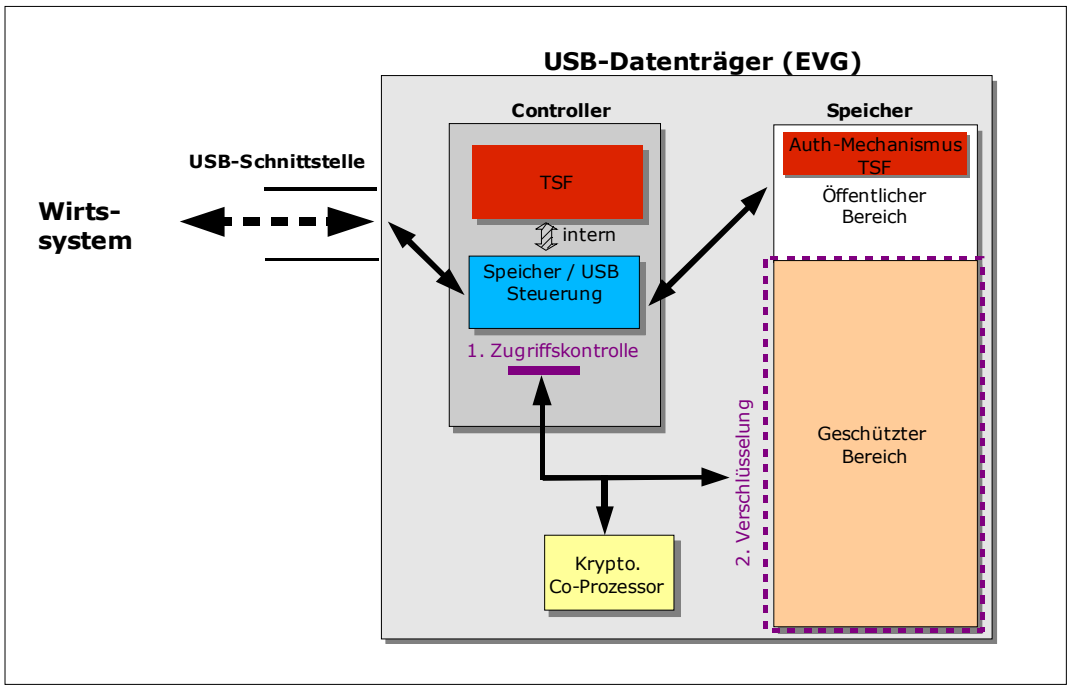
26 Der Evaluierungsgegenstand (EVG) bezieht sich auf Datenträger mit integrierter Sicherheitsfunktionalität zum Anschluss an die USB-Schnittstelle von Wirtssystemen.

> ***Anwendungsbemerkung 1*** *Die USB-Schnittstelle wird als Schnittstelle vorausgesetzt, da diese eine automatische Erkennung von USB-Peripheriegeräten im laufenden Betrieb ohne Installation von Software ermöglicht. Dadurch wird die Kapselung der Sicherheitsfunktionen im EVG selbst realisierbar.*

27 Das Schutzprofil geht nur soweit auf HW-Annahmen ein, wie diese unbedingt notwendig sind. Dadurch wird ein breites Spektrum an technischen Lösungen ermöglicht.

> ***Anwendungsbemerkung 2*** *Für den Anschluss an die USB-Schnittstelle stehen eine Vielzahl unterschiedlicher Datenträgertypen zur Verfügung. Die Datenträger unterscheiden sich in Speichertyp, Kapazität, Zugriffsgeschwindigkeit und Lebensdauer. Diese Kriterien sind für die Betrachtung im Schutzprofil nicht relevant.*

**Abbildung 1 Genereller Aufbau des EVGs**



28 In Abbildung 1 ist der generelle Aufbau eines USB-Datenträgers mit integrierter Sicherheitsfunktionalität dargestellt. Die für die Sicherheitsleistung relevanten Komponenten sind wie folgt definiert:

- Controller: Regelt den Informationsfluss innerhalb des EVGs und nach außen über die USB-Schnittstelle hin zum Wirtssystem. Der Controller steuert den Zugriff auf die Speicherbereiche des EVGs. Ausschließlich bei erfolgreicher Authentisierung etabliert der Controller eine Verbindung zum geschützten Speicherbereich.
- Speicher: Der Speicher enthält die Daten des EVGs. Er ist in zwei Speicherbereiche unterteilt:
  - Öffentlicher Speicherbereich: Auf diesen Speicherbereich kann ohne Authentisierung zugegriffen werden. Die Daten in diesem Bereich sind nicht verschlüsselt. Der öffentliche Bereich kann genutzt werden, um dem Benutzer ein Programm zur Eingabe des Authentisierungsmerkmals bereitzustellen (siehe Abbildung 1). Liegt das Programm zur Übertragung der Authentisierungsdaten an den Controller im öffentlichen Speicherbereich, ist dieser Teil des öffentlichen Speicherbereiches als TSF zu betrachten und muss schreibgeschützt sein.

    Sollte der öffentliche Bereich keine Sicherheitsfunktionen enthalten, muss er in der Speicherstruktur des EVGs nicht vorhanden sein. Ansonsten kann dieser Speicherbereich genutzt werden um nicht schützenswerte Daten abzulegen, auf die ohne Authentisierung zugegriffen werden soll.
  - Geschützter Speicherbereich: Dieser Speicherbereich enthält die vertraulichen Daten des Benutzers und wird deshalb durch die Sicherheitsfunktionen des EVGs geschützt. Zugriff auf den geschützten Speicher erhält der Benutzer erst nach erfolgreicher Authentisierung.

***Anwendungsbemerkung 3*** *Der öffentliche Bereich ist für die Betrachtung nur relevant, wenn dieser Teil den Authentisierungsmechanismus enthält. Anforderungen an die vertrauliche Speicherung von Daten richten sich ausschließlich an den geschützten Speicherbereich. Der geschützte Speicherbereich kann den gesamten Speicher des EVGs umfassen.*

- Kryptographischer Co-Prozessor: Wird zur Ausführung der Ver-/Entschlüsselungsprozesse im EVG genutzt. Durch den Einsatz eines kryptographischen Co-Prozessors laufen die Ver-/Entschlüsselungsprozesse vollständig im EVG selbst ab. Der kryptographische Co-Prozessor kann als eigenständiges Bauelement oder im Controller des EVGs realisiert sein. Ist der kryptographische Co-Prozessor als eigenständiges Bauelement realisiert, enthält dieser nicht

den vollständigen kryptographischen Schlüssel zur Entschlüsselung der Daten.

29

***Anwendungsbemerkung 4*** *Würde der krypto. Co-Prozessor den vollständigen Schlüssel enthalten, wäre es möglich durch eine Übertragung eines unberechtigten Entschlüsselungsbefehls die Entschlüsselung der Daten zu veranlassen. Ein unberechtigter Entschlüsselungsbefehl könnte z.B. über einen ausgetauschten Controller erzeugt werden.*

30 Der EVG gewährleistet die Vertraulichkeit der Daten im geschützten Bereich durch zwei unterschiedliche Sicherheitsmechanismen:

- Zugriffskontrolle
- Verschlüsselung

31 Zugriffskontrolle: Der Controller des EVGs etabliert eine Verbindung zum geschützten Speicherbereich erst nach vorheriger erfolgreicher Authentisierung durch den Benutzer. Zugriffsversuche ohne erfolgreiche Authentisierung werden auf Hardware-Ebene des EVGs geblockt.

32 Verschlüsselung: Der zweite Sicherheitsmechanismus des EVGs ist die Verschlüsselung der Daten im geschützten Speicherbereich. Die Verschlüsselung stellt speziell bei physischen Angriffen auf den Speicher die Vertraulichkeit der Daten sicher.

33 Ein wesentliches Merkmal des EVGs ist die vollständige Implementierung der Sicherheitsfunktionen im EVG selbst (siehe Abbildung 1). Durch diese Konzeption wird eine Verfügbarkeit der vertraulichen Daten an jedem Wirtssystem ermöglicht. Der EVG ist unabhängig von der Konfiguration des Wirtssystems. Eine Inbetriebnahme des EVGs erfordert keine vorinstallierte Sicherheitssoftware auf dem Wirtssystem. Es werden lediglich eine USB-Schnittstelle und ein schnittstellenkompatibles Betriebssystem vorausgesetzt.

34 Nach Anschluss des EVGs an das Wirtssystem muss sich der Benutzer authentisieren, um Zugriff auf die Daten im geschützten Speicherbereich nehmen zu können. Der Controller steuert die beiden Sicherheitsmechanismen Zugangskontrolle und Verschlüsselung. Der Authentisierungsmechanismus überträgt das Authentisierungsmerkmal an den Controller. Die Korrektheit des Authentisierungsmerkmals wird vom Controller überprüft. Ist die Authentisierung erfolgreich, etabliert der Controller eine logische Verbindung zum geschützten Speicherbereich und die Daten werden entschlüsselt Die Authentisierung durch den Benutzer muss nur einmal pro Sitzung erfolgen.

***Anwendungsbemerkung 5*** *Das Schutzprofil stellt keine Anforderung an die technische Realisierung des Authentisierungsmechanismus zur Eingabe des Authentisierungsmerkmals. Die Authentisierung kann z.B. über Tastatureingabe oder über einen Fingerabdruckscanner direkt am EVG erfolgen. Treten mehrfach fehlgeschlagene Authentisierungsversuche auf, sollte der EVG mit Zeitverzögerungen reagieren. Ab einer bestimmten Anzahl fehlgeschlagener Authentisierungsversuche könnte die Reaktion des EVGs auch eine Vernichtung der vertraulichen Daten sein, da es sich vermutlich um einen Penetrationsangriff handelt.*

35 Der EVG ist auf eine anwenderfreundliche Bedienung ausgelegt. Abgesehen von der erforderlichen Authentisierung zu Beginn unterscheidet sich die Arbeit mit dem EVG nicht von der mit einem ungesicherten Datenträger. Nach der Authentisierung kann der Benutzer auf das Dateisystem des EVGs über das Wirtssystem zugreifen.

36 Die Verschlüsselungsprozesse laufen für den Benutzer transparent im Hintergrund ab. Nach erfolgreicher Authentisierung wird nicht der gesamte Inhalt des geschützten Speicherbereichs entschlüsselt. Es werden immer nur die Daten entschlüsselt und zum Wirtssystem übertragen, die für die anstehende Aktion benötigt werden.

37 Bei Störungen der logischen Verbindung wie z.B. ein Systemabsturz, ein Stromausfall oder Trennung der physikalischen Verbindung zwischen EVG und Wirtssystem, sorgt der EVG dafür, dass Daten im Speicher verschlüsselt bleiben und das Dateisystem nicht beschädigt wird. Nach einer Störung erlangt der EVG wieder einen stabilen und konsistenten Zustand. Alle Sicherheitsmechanismen des EVGs sind wieder aktiviert. Eine Wiederauthentisierung durch den Benutzer ist erforderlich, um erneut auf die Daten des geschützten Speicherbereichs zuzugreifen.

***Anwendungsbemerkung 6*** *Vorteilhaft für den Benutzer wäre auch das Vorhandensein einer Schreibschutzfunktion im EVG. Diese Funktion könnte nach Aktivierung (z.B. durch das Umlegen eines mechanischen Schalters am EVG-Gehäuse) die Daten im geschützten Speicherbereich mit einem Schreibschutz versehen. Diese Funktion würde mögliche Angriffe vom Wirtssystem auf die Integrität der vertraulichen Daten abwehren.*

## 2.2 Abgrenzung des Evaluierungsgegenstandes

38 Bei dem betrachteten EVG handelt es sich um einen Datenträger mit integrierter Sicherheitsfunktionalität. Für die Evaluierung sind die Komponenten: öffentlicher Speicherbereich, geschützter Speicherbereich, Controller, kryptographischer Co-Prozessor und die USB-Schnittstelle relevant.

39 Die USB-Schnittstelle ist die einzige externe Schnittstelle des EVGs. Zur Nutzung des EVGs wird dieser über die USB-Schnittstelle an ein Wirtssystem

angeschlossen. Die gesamte Sicherheitsleistung wird vom EVG selbst erbracht. Die TSF sind im Controller des EVGs implementiert, es können aber auch Teile der TSF im öffentlichen Speicherbereich implementiert sein. Das Wirtssystem ist nicht Teil der Evaluierung.

40 Der EVG verfügt über einen kryptographischen Co-Prozessor, dieser wird zur Ausführung der Ver-/Entschlüsselungsprozesse genutzt. Der kryptographische Schlüssel verlässt in keinen Fall den EVG.

41 Der EVG kann nicht kontrollieren ob Datenspuren auf dem Wirtssystem zurückbleiben, die Rückschlüsse auf vertrauliche Daten des EVGs erlauben. Datenspuren entstehen bei der Nutzung von Anwendungen im Zusammenhang mit den Daten des EVGs. In diesem Kontext kann auch die sogenannte Papierkorb-Funktion eine Gefahr darstellen.

> ***Anwendungsbemerkung 7*** *Dieses Schutzprofil soll u.a. auf die Problematik der Datenspuren aufmerksam machen. Es ist nicht abzusehen, welche Datenspuren auf dem Wirtssystem entstehen, darüber hat der EVG keine Kontrolle. Aus diesem Grund enthält das Schutzprofil keine Anforderungen an den EVG im Zusammenhang mit Datenspuren. Der PP-Verfasser empfiehlt im EVG Funktionen zur Entfernung von typischen Datenspuren gängiger Betriebssysteme zu implementieren. Oder entsprechende Software mitzuliefern. Auch durch Hinweise im Benutzerhandbuch zur Problematik von Datenspuren könnte man die Gefahr verringern.*

## 2.3 Technische Flexibilität

42 Dieses Schutzprofil richtet sich an die gesamte Produktklasse USB-Datenträger. Die Anforderungen dieses Schutzprofils sind so flexibel wie möglich spezifiziert, um eine Evaluierung unterschiedlicher technischer Implementierungen von USB-Datenträgern zu ermöglichen.

43 Im Folgenden werden die wichtigsten Aspekte hinsichtlich der Implementierungsunabhängigkeit aufgelistet:

- Authentisierungsmechanismus: Es wird kein spezifischer Authentisierungsmechanismus vorausgesetzt. Die Authentisierung kann z.B. über ein Passwort oder biometrische Daten erfolgen.
- Speicherstruktur: Die Struktur des Speichers wurde bis auf die Forderung eines geschützten Speicherbereichs offen gelassen. Der Speicher kann beispielsweise einen öffentlichen Speicherbereich enthalten.
- Platzierung des kryptographischen Co-Prozessors:: Der kryptographische Co-Prozessor kann innerhalb des Controller oder als eigenständiges Bauelement im EVG realisiert sein.
- Kryptographische Algorithmus: Es wird kein spezifischer kryptographischer Algorithmus gefordert. Die Auswahl des konkreten kryptographischen Algorithmus bleibt dem Hersteller und somit dem ST-Autor überlassen.

- Kryptographischer Schlüssel: Die Generierung des kryptographischen Schlüssels ist offen gelassen. Dieser kann z.B. aus dem Authentisierungsmerkmal generiert werden. Ferner ist es beispielsweise möglich, dass der kryptographische Schlüssel bei der Fertigung des Controllers generiert und in den Controller integriert wird.

## 2.4 Einsatzszenarien / EVG-Verwendung

44 In den folgenden beispielhaft aufgeführten Szenarien für den Einsatz von Datenträgern, wird speziell der Umgang mit vertraulichen Daten betrachtet. Die Szenarien zeigen typische Einsatzgebiete, in denen der EVG zum Schutz vertraulicher Daten eingesetzt werden sollte.

**45 Datentransport**

46 Datentransport, d. h. Transport vertraulicher Daten über einen Datenträger zwischen Wirtssystemen. Typische Szenarien im Geschäftsumfeld die einen Transport vertraulicher Daten erfordern sind Projektbesprechungen, Präsentationen beim Kunden oder Geschäftsreisen. Auch im privaten Umfeld werden häufig vertrauliche Daten über Datenträger transportiert, z.B. Präsentation persönlicher Multimedia oder Vorlage von Daten beim Steuerberater.

**47 Transport der Arbeitsumgebung (Profiltransport)**

48 Neben den vertraulichen Nutzdaten wird die Arbeitsumgebung eines Benutzers auf einem Datenträger transportiert. Wird der Datenträger an ein Wirtssystem angeschlossen, passt sich die Arbeitsumgebung des Systems an das Profil des Benutzers an. Das Profil enthält z.B. das Hintergrundbild, die Anordnung der Symbole und die Internet-Favoriten des Benutzers.

49 Die Datenträger verfügen über ausreichend Kapazität und Leistung um komplette, fertig konfigurierte Anwendungen wie Office-Pakete, Webbrowser und E-Mail-Clients zu transportieren. Diese Anwendungen sind Teil der Arbeitsumgebung und werden direkt vom Datenträger gestartet, es ist keine Installations-CD notwendig. Somit steht dem Benutzer am Wirtssystem seine gewohnte Arbeitsumgebung samt Anwendungen zur Verfügung. Der Transport der Arbeitsumgebung kann sich auch auf den Transport der bereits konfigurierten Anwendungen beschränken.

**50 Datensicherung**

51 Unter dem Vorgang der Datensicherung versteht man das Kopieren der in einem Wirtssystem vorhandenen vertraulichen Daten auf einen Datenträger. Die Datensicherung dient dem Schutz vor Datenverlust durch z.B. Hardware-Schäden, Diebstahl, versehentliches oder absichtliches Löschen. Der Datenträger enthält eine Kopie der wichtigen und vertraulichen Daten des Wirtssystems.

**52** **Schlüsselspeicher**

53 Der Datenträger wird zur Speicherung vertraulicher Schlüssel oder digitaler Zertifikate verwendet. Wird ein Schlüssel benötigt z.B. zur Verschlüsselung einer E-Mail-Nachricht wird der Datenträger mit dem Wirtssystem verbunden. Die Anwendung benutzt den Schlüssel vom Datenträger für die anstehende Aktion. Anschließend wird der Datenträger vom System getrennt und sicher gelagert. Viele asymmetrische Verschlüsselungsverfahren wie PGP empfehlen das Auslagern des privaten Schlüssels auf einen externen Datenträger.

## 2.5 Datenarten

54 Um einen Eindruck der zu schützenden Daten zu vermitteln, werden hier beispielhaft einige aufgeführt:

**55** **Unternehmensdaten**

- Präsentationen,
- Geschäftspläne,
- Auslagerungen / Backups (bspw. E-Mail Backup)
- Finanz , Personal-, Kunden-, Wartungsdaten
- Vertrauliche E-Mail
- Zugangsdaten für das Firmennetzwerk

**56** **Private Daten**

- Passwörter, PINs,
- Briefe, E-Mail,
- vertraulicher Webzugang z. B. für Webbanking,
- Konto/Depotauszüge,
- Adressbuch, Terminkalender,
- Persönliche Multimedia (Bilder, Videos,..)

**57** **Software und Schlüssel**

- Programme,
- Module,
- Algorithmen,
- Schlüsseldaten (PIN, Passwörter, PGP Key Chain)

# 3 EVG-Sicherheitsumgebung

58 Dieses Kapitel beschreibt Annahmen an die Umgebung, in der der Evaluationsgegenstand eingesetzt werden soll, die damit Auflagen an den Betrieb darstellen. Des Weiteren werden alle vom EVG abzuwehrenden Bedrohungen aufgeführt.

## 3.1 Rollen im EVG

59 Es gibt die folgenden, im Kontext des Evaluationsgegenstands zu berücksichtigenden Rollen mit den nachfolgend aufgeführten möglichen Aktivitäten (Für eine detaillierte Aufführung der zulässigen Aktivitäten sei auf die Definition der funktionalen Sicherheitspolitik in Abschnitt 5.1.1 verwiesen.):

- Autorisierter Benutzer (S1)
  - Ist im Besitz des Authentisierungsmerkmals zum Zugriff auf den geschützten Speicherbereich des EVGs, in dem die vertraulichen Daten gespeichert sind.
  - Kann das Authentisierungsmerkmal modifizieren.

- Nicht autorisierter Benutzer (S2)
  - Ist interessiert an den vertraulichen Daten von S1, die im Speicher des USB-Datenträgers liegen (Beispiele für vertrauliche Daten sind in Kapitel 2.5 aufgeführt).
  - Verfügt nicht über das Authentisierungsmerkmal für den Zugriff auf die geschützten Daten.
  - Verfügt über die Möglichkeit, sich einen baugleichen USB-Datenträger zu beschaffen. An diesem USB-Datenträger kann er sowohl logische als auch physische Angriffe erproben.
  - Durch die kompakte Bauweise des EVGs ist es für S2 relativ einfach, in den Besitz des EVGs zu gelangen.

## 3.2 Annahmen

60 Im Abschnitt Annahmen werden die Sicherheitsauflagen an die Umgebung angeführt, in der der Evaluationsgegenstand eingesetzt werden soll und deren Umsetzung angenommen wird. Dieser Abschnitt kann als Auflagenkatalog an den Betreiber des EVGs angesehen werden. Jeder Annahme wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben A (von engl. „Assumption") zugeordnet.

61 Eine Begründung für die Annahmen findet sich im Erklärungsteil dieses Schutzprofils in Abschnitt 6.3.

62 A.Ausspähen S1 achtet darauf, dass sein Authentisierungsmerkmal nicht ausgespäht werden kann. Das betrifft z.B. das Mitlesen des Passworts oder die Reproduktion des biometrischen Authentisierungsmerkmals.

> ***Anwendungsbemerkung 8*** *S1 kann kaum vermeiden, dass er biometrische Spuren hinterlässt (z.B. Fingerabdrücke), die zur Reproduktion seines biometrischen Authentisierungsmerkmals genutzt werden könnten. Die Annahme A.Ausspähen soll verdeutlichen, dass die Möglichkeit der Reproduktion eines biometrischen Authentisierungsmerkmals eine potenzielle Gefahr darstellt.*

63 A.Vertrau.WS Nach Freigabe des geschützten Speicherbereichs durch S1, erfolgen vom Wirtssystem und einem eventuell angeschlossen Netzwerk keine unerlaubten Zugriffe auf den EVG.

64 A.Abwesend Verlässt S1 das Wirtssystem, an das der zuvor freigegebene EVG angeschlossen ist, so trifft er geeignete Maßnahmen um die Daten in seiner Abwesenheit zu schützen. Geeignete Maßnahmen können z.B. eine Arbeitsplatzsperrung über das Betriebssystem oder die Mitnahme des EVGs sein.

## 3.3 Bedrohungen

65 Im Abschnitt Bedrohungen werden alle Bedrohungen als konkrete Ereignisse aufgeführt, die der EVG selbst abzuwehren hat. Jeder Bedrohung wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben T (von engl. „Threat“) zugeordnet.

66 T.logZugriff Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, greift er auf die vertraulichen Daten des EVGs zu. Den logischen Zugriff erlangt S2 beispielsweise, indem er den EVG an die USB-Schnittstelle eines Computersystems anschließt.

67 T.phyZugriff Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, greift er über eine physische Attacke auf den Speicher des EVGs zu. Eine physische Attacke könnte z.B. folgendes Szenario sein: Der Speicher des EVGs wird durch S2 entnommen. Nach der Entnahme wird der Speicher in einen anderen USB-Datenträger eingesetzt, über den S2 logisch auf den Speicher zugreift.

68 T.AuthÄndern Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, setzt er ein neues Authentisierungsmerkmal. Infolgedessen werden die Daten für S1 unbrauchbar.

69 T.Störung Durch eine Störung (z.B. Stromausfall oder Betriebssystemfehler) wird der korrekte Betrieb des EVGs gestört. Als Ergebnis bleiben vertrauliche Daten unverschlüsselt oder das Dateisystem des EVGs wird beschädigt.

## 3.4 Organisatorische Sicherheitspolitiken (OSP)

70 Im Abschnitt Organisatorische Sicherheitspolitiken werden die relevanten Gesetze, deren Einhaltung der EVG zu erzwingen oder zu unterstützen hat, aufgeführt.

71 In diesem Schutzprofil werden keine organisatorischen Sicherheitspolitiken vorgegeben, da alle Motivation zur IT-Sicherheitsfunktionalität implizit in Form von abzuwehrenden Bedrohungen dargestellt ist.

# 4 Sicherheitsziele

72 Dieses Kapitel legt produktunabhängig dar, wie der EVG den zuvor genannten Bedrohungen begegnet. Jedem Sicherheitsziel wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben O (von engl. „Objective“) zugeordnet.

## 4.1 EVG-Sicherheitsziele

73 O.logZugriff Der EVG muss einen sicheren Authentisierungsmechanismus bereitstellen, über den ausschließlich S1, durch eine erfolgreiche Authentisierung, Zugriff auf die geschützten Daten erhält.

74 O.phyZugriff Der EVG verschlüsselt alle Daten im geschützten Bereich des EVGs. Die Verschlüsselung sichert speziell im Fall physischer Attacken auf den EVG den Schutz der Vertraulichkeit.

75 O.AuthÄndern Der EVG bietet eine Funktion zur Änderung des Authentisierungsmerkmals ausschließlich nach vorheriger erfolgreicher Authentisierung durch S1.

76 O.Störung Der EVG erlangt nach einer Störung (z.B. Stromausfall) wieder einen stabilen und konsistenten Zustand. Die Störung führt weder zu einer Schädigung des Dateisystems noch bleiben Daten unverschlüsselt im Speicher des EVGs.

## 4.2 Sicherheitsziele für die IT-Umgebung

***Anwendungsbemerkung 9*** *Als IT-Umgebung wird das jeweilige Wirtssystem betrachtet, an das der EVG im Betrieb angeschlossen ist.*

77 OE.Vertrau.WS Der EVG kann sich nach Freigabe des geschützten Speicherbereichs nicht gegen unerlaubte Zugriffe vom Wirtssystem schützen. Daher erfolgen über das Wirtssystem und einem eventuell angeschlossen Netzwerk keine unerlaubten Zugriffe z.B. durch Schadsoftware auf den EVG.

78 OE.Abwesend Nach Freigabe der Daten kann auf diese ungehindert zugegriffen werden, solange der EVG am Wirtssystem angeschlossen ist. Deshalb muss S1 für den Zeitraum seiner Abwesenheit vom Wirtssystem geeignete Sicherheitsmaßnahmen treffen, um den Zugriff von S2 auf die zuvor freigegebenen Daten auf dem EVG zu verhindern.

## 4.3 Sicherheitsziele für die Nicht-IT-Umgebung

79 OE.Ausspähen Der EVG kann reproduzierte Authentisierungsmerkmale nicht erkennen. Daher muss S1 darauf achten, dass sein Authentisierungsmerkmal nicht mitgelesen oder reproduziert werden kann.

# 5 IT-Sicherheitsanforderungen

80 Dieses Kapitel beinhaltet funktionale Sicherheitsanforderungen an den EVG und Vertrauenswürdigkeitsanforderungen and den EVG und seine Umgebung.

81 Die funktionalen Sicherheitsanforderungen sind im Abschnitt 5.1 „Funktionale Sicherheitsanforderungen an den EVG“ definiert. Die funktionalen Sicherheitsanforderungen entstammen aus Teil 2 der CC [CC-Teil2]. Der Teil 2 enthält einen Katalog von Sicherheitsanforderungen in Form von semiformalen Textbausteinen genannt „Komponenten“. Jede Komponente wird dort mit ihrer Funktionalität, Einsatzvoraussetzung sowie ihrer Abhängigkeit zu anderen Sicherheitsanforderungen beschrieben. Die Komponenten können durch definierte Operationen angepasst werden.

82 Die Vertrauenswürdigkeitsanforderungen sind in Abschnitt REFFORMATVERBINDEN5.3 „Anforderungen an die Vertrauenswürdigkeit des EVGs“ definiert. Diese Anforderungen entstammen Teil 3 der CC [CC-Teil3]. Diese Anforderungen dienen zur Überprüfung der Korrektheit der Implementation eines Produktes.

**83** **Schreibweise**[T1]

Kennzeichnung der Operationen:

- Die Operationen „Zuweisung“ und „Auswahl“ sind *kursiv* dargestellt
- Die Operation „Verfeinerungen“ ist <u>unterstrichen</u> dargestellt.
- Sind die Operationen „Zuweisung“ und „Auswahl“ offen gelassen, so ist der enthaltende Text nicht formatiert.

84 Jeder Text innerhalb der Komponenten, die in Abschnitt 5.1 aufgeführt sind, der weder *kursiv* noch <u>unterstrichen</u> gedruckt ist, entspricht dem Originaltext der jeweiligen Komponente aus Teil 2 der CC.

## 5.1 Funktionale Sicherheitsanforderungen an den EVG

### 5.1.1 Definition der funktionalen Sicherheitspolitik für USB-Datenträger

85 Bevor die funktionalen Sicherheitsanforderungen an den EVG aufgeführt werden, wird die **funktionale Sicherheitspolitik für USB-Datenträger (FSUD)** wie folgt definiert:

- zulässige Aktionen des autorisierten Benutzers (S1):
  - Benutzung des Authentisierungsmechanismus
  - Lesen / Schreiben / Modifizieren der Daten im öffentlichen und im geschützten Speicherbereich des EVGs (Zugriff erlauben)
  - Erneute Authentisierung nach Verbindungsstörung zwischen Wirtssystem und EVG (z.B. durch physikalische Trennung, Stromverlust oder Betriebssystemfehler)
  - Modifizieren des Authentisierungsmerkmals
- zulässige Aktionen des nicht autorisierten Benutzers (S2)
  - Lesen / Schreiben / Modifizieren der Daten im öffentlichen Speicherbereich (falls vorhanden)
  - Benutzung des Authentisierungsmechanismus

### 5.1.2 Funktionale Sicherheitsanforderungen an den EVG

86 Im Folgenden werden die funktionalen Sicherheitsanforderungen für den EVG dargestellt.

**Tabelle 1: fasst die aus Teil 2 der CC entnommenen funktionalen Anforderungen dieses Schutzprofils zusammen.**

| | |
|---|---|
| FCS_CKM.1 | Kryptographische Schlüsselgenerierung |
| FCS_CKM.4 | Zerstörung des kryptographischen Schlüssels |
| FCS_COP.1 | Kryptographischer Betrieb |
| FDP_ACC.1 | Teilweise Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| FIA_SOS.1 | Verifizierung von Geheimnissen |
| FIA_UAU.1 | Zeitpunkt der Authentisierung |
| FIA_UAU.6 | Wiederauthentisierung |
| FMT_MSA.1 | Management der Sicherheitsattribute |
| FMT_SMF.1 | Spezifikation der Management Funktionen |
| FMT_SMR.1 | Sicherheitsrollen |

| | |
|---|---|
| FPT_FLS.1 | Erhaltung eines des sicheren Zustandes bei Fehlern |
| FPT_RCV.4 | Funktionelle Wiederherstellung |

#### 5.1.2.1 Kryptographische Unterstützung (FCS)

**87 FCS_CKM.1 Kryptographische Schlüsselgenerierung**

88 Ist hierarchisch zu: Keinen anderen Komponenten.

89 FCS_CKM.1.1 Die TSF müssen die kryptographischen Schlüssel gemäß eines spezifizierten Algorithmus zur kryptographischen Schlüsselgenerierung [Zuweisung: Algorithmus zur kryptographischen Schlüsselgenerierung] und spezifizierte kryptographische Schlüssellängen [Zuweisung*:* kryptographische Schlüssellängen], die den folgenden [Zuweisung: Liste der Normen] entsprechen, generieren.

90 Abhängigkeiten:

[FCS_CKM.2 Verteilung des kryptographischen Schlüssels oder FCS_COP.1 Kryptographischer Betrieb]FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

FMT_MSA.2 Sichere Sicherheitsattribute

**91 FCS_CKM.4 Zerstörung des kryptographischen Schlüssels**

92 Ist hierarchisch zu: Keinen anderen Komponenten.

93 FCS_CKM.4.1 Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Zerstörung des kryptographischen Schlüssels [Zuweisung: Methode zur Zerstörung des kryptographischen Schlüssels], die den folgenden [Zuweisung: Liste der Normen] entspricht, zerstören.

94 Abhängigkeiten:

[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung]

FMT_MSA.2 Sichere Sicherheitsattribute

**95 FCS_COP.1 Kryptographischer Betrieb**

96 Ist hierarchisch zu: Keinen anderen Komponenten.

97 FCS_COP.1.1 Die TSF müssen [Zuweisung: *die Ver- und Entschlüsselung der Daten im geschützten Speicherbereich des EVGs*] gemäß eines spezifizierten kryptographischen Algorithmus *[*Zuweisung: kryptographischer Algorithmus] und kryptographischer Schlüssellängen [Zuweisung: kryptographische Schlüssellänge], die den folgenden [Zuweisung: Liste der Normen] entsprechen, durchführen.

98 Abhängigkeiten:

[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung]

FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

FMT_MSA.2 Sichere Sicherheitsattribute

#### 5.1.2.2 Identifikation und Authentisierung (FIA)

**99 FIA_UAU.1 Zeitpunkt der Authentisierung**

100 Ist hierarchisch zu: keiner anderen Komponente

FIA_UAU.1.1 Die TSF müssen die Ausführung des [Zuweisung: Zugriffs *auf den öffentlichen Speicherbereich*] für den Benutzer erlauben, bevor dieser authentisiert wird.

101 FIA_UAU.1.2 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

102 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

***Anwendungsbemerkung 10*** *Sollte kein öffentlicher Speicherbereich vorhanden sein , kann FIA_UAU.1 durch FIA_UAU.2 ersetzt werden.*

***Anwendungsbemerkung 11*** *Der betrachtete EVG ist ein Single-User-System, daher ist keine Identifizierung notwendig. Es existiert nur ein Authentisierungsmerkmal, das Zugriff auf die Daten im geschützten Speicherbereich ermöglicht. Vorstellbar wäre auch ein EVG, auf dem mehrere Benutzer jeweils ihren eigenen Speicherbereich im EVG hätten.*

**103 FIA_UAU.6 Wiederauthentisierung**

104 Ist hierarchisch zu: Keinen anderen Komponenten.

105 FIA_UAU.6.1 Die TSF müssen den Benutzer unter den Bedingungen [Zuweisung: *Systemabsturz, Stromausfall, Trennung der physischen Verbindung oder einer anderen Verbindungsstörung]* wiederauthentisieren.

106 Abhängigkeiten: Keine Abhängigkeiten

***Anwendungsbemerkung 12*** *Die Operation Zuweisung der folgenden funktionalen Komponente FIA_SOS.1 ist auf Qualitätsmetriken eingeschränkt, die die Anforderungen der Stärke SOF-mittel erfüllen.*

**107 FIA_SOS.1 Verifizierung von Geheimnissen**

108 Ist hierarchisch zu: Keinen anderen Komponenten.

109 FIA_SOS. 1 Die TSF müssen einen Authentisierungsmechanismus bereitstellen, um zu verifizieren, dass das Authentisierungsmerkmal der [Zuweisung: *definierte Qualitätsmetrik*] entspricht.

Abhängigkeiten: Keine Abhängigkeiten

#### 5.1.2.3 Schutz der Benutzerdaten (FDP)

**110 FDP_ACC.1 Teilweise Zugriffskontrolle**

111 Ist hierarchisch zu: keiner anderen Komponente

112 FDP_ACC.1.1 Die TSF müssen die [Zuweisung: *FSUD*] für [Zuweisung: *den Zugriff von S1 auf die Daten im geschützten Speicherbereich des EVGs*] durchsetzen.

**113** Abhängigkeiten: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen.

***Anwendungsbemerkung 13*** *Sollte kein öffentlicher Speicherbereich vorhanden sein, kann FDP_ACC.1 durch FDP_ACC.2 ersetzt werden.*

**114 FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen**

***Anwendungsbemerkung 14*** *Der Text der Komponente FDP_ACF.1.1 wurde nach der Final Interpretation RI # 103 angepasst und ins Deutsche übersetzt.*

115 Ist hierarchisch zu: Keinen anderen Komponenten.

116 FDP_ACF.1.1 Die TSF müssen die [Zuweisung: FSUD] für Objekte , basierend auf dem Folgenden durchsetzen: [Zuweisung:

| Subjekt | Objekt | Sicherheitsattribut |
|---|---|---|
| S1 | Geschützter Speicherbereich | Authentisierungs-merkmal |

],

117 FDP_ACF.1.2 Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist: [Zuweisung:

- *zulässige Aktionen des autorisierten Benutzers (S1):*
  - *Benutzung des Authentisierungsmechanismus*
  - *Lesen / Schreiben / Modifizieren der Daten im öffentlichen und im geschützten Speicherbereich des EVGs (Zugriff erlauben)*
  - *Erneute Authentisierung nach Verbindungsstörung zwischen Wirtssystem und EVG (z.B. durch physikalische Trennung, Stromverlust oder Betriebssystemfehler)*
  - *Modifizieren des Authentisierungsmerkmals*
- *zulässige Aktionen des nicht autorisierten Benutzers (S2)*
  - *Lesen / Schreiben / Modifizieren der Daten im öffentlichen Speicherbereich (falls vorhanden)*
  - *Benutzung des Authentisierungsmechanismus*

*].*

118 FDP_ACF.1.3 Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln explizit autorisieren: [Zuweisung: *keine Regeln*].

119 FDP_ACF.1.4 Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf [Zuweisung: *keine Regeln*], explizit verweigern.

120 Abhängigkeiten: FDP_ACC.1 Teilweise Zugriffskontrolle

FMT_MSA.3 Initialisierung statischer Attribute

#### 5.1.2.4 Sicherheitsmanagement (FMT)

121

***Anwendungsbemerkung 15*** *Die Abhängigkeiten der folgenden Komponente wurden entsprechend der Final Interpretation RI # 65 angepasst.*

122 **FMT_MSA.1 Management der Sicherheitsattribute**

123 Ist hierarchisch zu: Keinen anderen Komponenten.

124 FMT_MSA.1.1 Die TSF müssen die [Zuweisung: *FSUD*] zur Beschränkung der Fähigkeit zum [Auswahl: *Modifizieren,* [Zuweisung: *keine anderen Operationen*]] des Sicherheitsattributs [Zuweisung: *Authentisierungsmerkmal*] auf [Zuweisung: *S1*] durchsetzen.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder

FDP_IFC.1 Teilweise Informationsflußkontrolle]

FMT_SMR.1 Sicherheitsrollen

FMT_SMF.1 Spezifikation der Management Funktionen

***Anwendungsbemerkung 16*** *Die folgende funktionale Komponente FMT_SMF.1 ergibt sich aus der Final Interpretation RI # 65 und wurde ins Deutsche übersetzt.*

125 **FMT_SMF.1 Spezifikation der Management Funktionen**

126 Ist hierarchisch zu: Keinen anderen Komponenten.

127 FMT_SMF.1.1 Die TSF müssen die Fähigkeit besitzen folgende Sicherheitsmanagementfunktionen durchzuführen [Zuweisung: *modifizieren des Authentisierungsmerkmals*]

128 Abhängigkeiten: Keine Abhängigkeiten

**129 FMT_SMR.1 Sicherheitsrollen**

130 Ist hierarchisch zu: Keinen anderen Komponenten.

131 FMT_SMR.1.1 Die TSF müssen die Rollen [*Zuweisung: autorisierter Benutzer (S1)*] erhalten.

132 FMT_SMR.1.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

133 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

### 5.1.2.5 Schutz der TSF (FPT)

134 **FPT_FLS.1 Erhaltung des sicheren Zustandes bei Fehlern**

135 Ist hierarchisch zu: Keinen anderen Komponenten.

136 FPT_FLS.1.1 Die TSF müssen einen sicheren Zustand bei Auftreten folgender Fehlerarten: [Zuweisung: *Systemabsturz, Stromausfall, Trennung der physischen Verbindung, oder eine andere Verbindungsstörung*] erhalten.

137 Abhängigkeiten: ADV_SPM.1 Informelles EVG-Sicherheitsmodell

138 **FPT_RCV.4 Funktionelle Wiederherstellung**

139 Ist hierarchisch zu: Keinen anderen Komponenten.

140 FPT_RCV.4.1 Die TSF müssen sicherstellen, dass die [Zuweisung: *[Zuweisung: Liste der SF] im Falle Systemabsturz, Stromausfall, Trennung der physischen Verbindung oder einer anderen Störung]* die Eigenschaft besitzt, dass die SF entweder erfolgreich abgeschlossen wird, oder für die im Fall aufgeführten Fehlerszenarien, diese bis zu einem konsistenten und sicheren Zustand wiederherzustellen.

141 Abhängigkeiten: ADV_SPM.1 Informelles EVG-Sicherheitsmodell

#### 5.1.2.6 Abhängigkeiten der funktionalen Sicherheitsanforderungen

142 Tabelle 2 enthält eine Aufstellung der Abhängigkeiten der für den EVG ausgewählten funktionalen Komponenten der CC.

143 Die für das Schutzprofil ausgewählten funktionalen Komponenten sind in nachfolgender Tabelle durchnummeriert dargestellt. Sofern eine Komponente die Abhängigkeit von einer anderen Komponente beinhaltet, ist diese Komponente in der dritten Spalte der Tabelle aufgeführt. In der vierten Tabellenspalte kann die Nummer der Komponente abgelesen werden, die die entsprechende Abhängigkeit auflöst.

**Tabelle 2: Abhängigkeiten zwischen funktionalen Komponenten**

| Nr. | Funktionale Sicherheitsanforderungen | Abhängigkeiten | Bemerkung |
|---|---|---|---|
| 1 | FCS_CKM.1 | FCS_CKM.2 oder FCS_COP.1 | Aufgelöst in 3 |
| | | FCS_CKM.4 | Aufgelöst in 2 |
| | | FMT_MSA.2 | Nicht erforderlich (siehe 5.1.2.7):<br>- Der kryptographische Schlüssel besitzt keine Sicherheitsattribute |
| 2 | FCS_CKM.4 | FDP_ITC.1 oder<br>FDP_ITC.2 oder<br>FCS_CKM.1 | Aufgelöst in 1 |
| | | FMT_MSA.2 | Nicht erforderlich (siehe 5.1.2.7):<br>- Der kryptographische Schlüssel besitzt keine Sicherheitsattribute |
| 3 | FCS_COP.1 | FDP_ITC.1 oder<br>FDP_ITC.2 oder<br>FCS_CKM.1 | Aufgelöst in 1 |
| | | FCS_CKM.4 | Aufgelöst in 2 |

| | | | |
|---|---|---|---|
| | | FMT_MSA.2 | Nicht erforderlich (siehe 5.1.2.7):<br>- Der kryptographische Schlüssel besitzt keine Sicherheitsattribute |
| 4 | FIA_UAU.1 | FIA_UID.1 | Nicht erforderlich (siehe 5.1.2.7 ):<br>- Der EVG unterscheidet nicht zwischen verschiedenen Benutzern, er kennt nur die Rolle S1. Daher ist keine Identifizierung erforderlich. |
| 5 | FIA_UAU.6 | | Keine Abhängigkeiten |
| 6 | FIA_SOS.1 | | Keine Abhängigkeiten |
| 7 | FDP_ACC.1 | FDP_ACF.1 | Aufgelöst in 8 |
| 8 | FDP_ACF.1 | FDP_ACC.1 | Aufgelöst in 7 |
| | | FMT_MSA.3 | Nicht erforderlich (siehe 5.1.2.7):<br>- Der EVG vergibt keine Standardwerte an Sicherheitsattribute. |
| 9 | FMT_MSA.1 | FDP_ACC.1 oder<br>FDP_IFC.1 | Aufgelöst in 7 |
| | | FMT_SMR.1 | Aufgelöst in 11 |
| | | FMT_SMF. 1 | Aufgelöst in 10 |
| 10 | FMT_SMF.1 | | Keine Abhängigkeiten |
| 11 | FMT_SMR.1 | FIA_UID.1 | Nicht erforderlich (siehe 5.1.2.7 ):<br>Der EVG unterscheidet nicht zwischen verschiedenen Benutzern, er kennt nur die Rolle S1. Daher ist keine Identifizierung erforderlich. |
| 12 | FPT_FLS.1 | ADV_SPM.1 | Erfüllt durch Anpassung der EAL-Stufe (siehe Kapitel 5.2) |
| 13 | FPT_RCV.4 | ADV_SPM.1 | Erfüllt durch Anpassung der EAL-Stufe (siehe Kapitel 5.2) |

#### 5.1.2.7 Begründung der nicht erfüllten Abhängigkeiten

Im folgenden Abschnitt werden die nicht erfüllten Abhängigkeiten der funktionalen Komponenten begründet (siehe Tabelle 2).

Zu 1,2 und 3: Die Abhängigkeit FMT_MSA.2 ist nicht erforderlich, da der krypotgraphische Schlüssel keine Sicherheitsattribute verwendet. Die Umsetzung des Sicherheitsziels O.phyZugriff erfordert keine Sicherheitsattribute für den kryptographischen Schlüssel.

> ***Anwendungsbemerkung 17*** *Sollte ein konkretes Produkt Sicherheitsattribute für den kryptographischen Schlüssel vorsehen muss das ST entsprechend mit der funktionalen Komponente FMT_MSA.2 angepasst werden.*

Zu 8: Der EVG vergibt keine Standardwerte für Sicherheitsattribute, daher ist die Abhängigkeit zur FMT_MSA.3 nicht erforderlich. Die Umsetzung der Sicherheitsziele O.logZugriff und O.AuthÄndern erfordert keine Vergabe von Standardwerten für Sicherheitsattribute.

> ***Anwendungsbemerkung 18*** *Sollte ein konkretes Produkt Standardwerte für Sicherheitsattribute vorsehen muss das ST entsprechend mit der funktionalen Komponente FMT_MSA.3 angepasst werden.*

Zu 4 und 11: Der EVG enthält nur eine Rolle, den autorisierten Benutzer (S1). Daher ist eine Unterscheidung zwischen verschiedenen Rollen über eine Identifikation gefordert in FIA_UID.1 nicht erforderlich. Die Umsetzung keines der definierten Sicherheitsziele ist von einer Identifikation abhängig.

## 5.2 Anforderungen an die Umgebung

144 Die Sicherheitsziele für die IT-Umgebung werden durch die folgenden Sicherheitsanforderungen abgedeckt.

145 RE.Vertrau.WS Das Wirtssystem besitzt die Eigenschaft, unerlaubte Zugriffe (z.B. durch Schadsoftware) über das Wirtssystem oder ein eventuell angeschlossenes Netzwerk auf den EVG zu verhindern.

146 RE.Abwesend Das Wirtssystem besitzt die Eigenschaft, den logischen Zugang zum EVG auf Anforderung von S1 zu blockieren oder zu trennen.

## 5.3 Anforderungen an die Vertrauenswürdigkeit des EVGs

147 Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in nachfolgender Tabelle (Tabelle 3: Maßnahmen zur Erfüllung von EAL2 mit Zusatz ADV_SPM.1) aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL2 aus Teil 3 [CC-Teil3] der Common Criteria.

**Tabelle 3: Maßnahmen zur Erfüllung von EAL2 mit Zusatz ADV_SPM.1**

| Anforderungen gemäß EAL2 | | Maßnahmen der Entwickler |
|---|---|---|
| Konfigurations-management | ACM_CAP.2 | Kennzeichnung des EVGs mit einem eindeutigen Verweisnamen und eindeutige Identifikation der Konfigurationsteile zum besseren Verständnis der Zusammensetzung des EVGs |
| Auslieferung und Betrieb | ADO_DEL.1 | Auslieferungsprozeduren des Entwicklers sind klar definiert und dokumentiert. |
| | ADO_IGS.1 | Installations-, Generierungs- und Anlaufprozeduren werden in der Dokumentation für den Administrator behandelt. |
| Entwicklung | ADV_FSP.1 | Funktionale Spezifikation der TSF und ihrer externen Schnittstellen in einem informellen Stil. |
| | ADV_HLD.1 | Dokumentation der TSF hinsichtlich der wesentlichsten Struktureinheiten (d.h. Teilsystemen) im Zusammenhang mit deren Funktionen. |
| | ADV_RCR.1 | Die verschiedenen TSF-Darstellungen (im konkreten Fall FSP und HLD) müssen übereinstimmen |
| | ADV_SPM.1 | Nachweis, dass die TSF die Sicherheitspolitik durchsetzen. |
| Handbücher | AGD_ADM.1 | Vom Entwickler muss ein Systemverwalterhandbuch bereitgestellt werden, das an die zuständige Person gerichtet ist. |
| | AGD_USR.1 | Vom Entwickler muss ein Benutzerhandbuch bereitgestellt werden. |
| Testen | ATE_COV.1 | Nachweis, dass die TSF anhand ihrer funktionalen Spezifikation getestet wurde. |
| | ATE_FUN.1 | Die TSF-Tests und deren Ergebnisse sind dokumentiert |
| | ATE_IND.2 | Der Evaluator muß unabhängige Tests durchführen. |

| Anforderungen gemäß EAL2 | | Maßnahmen der Entwickler |
|---|---|---|
| Schwachstellen bewertung | AVA_SOF.1 | Für die SoF-relevanten Mechanismen (Authentisierungsmechanismus ) wurde eine Analyse in Bezug auf SoF „mittel“ durchgeführt und dokumentiert. |
| | AVA_VLA.1 | Eine Analyse wurde für alle offensichtlichen Schwachstellen des EVGs durchgeführt und dokumentiert. |

148 Die EAL-Stufe 2 wurde um die Komponente ADV_SPM.1 augmentiert. Die Erweiterung ergibt sich aus den Abhängigkeiten der funktionalen Sicherheitsanforderungen:

- FPT_FLS.1 Erhaltung des sicheren Zustandes bei Fehlern
- FPT_RCV.4 Funktionelle Wiederherstellung

Durch die Erweiterung ergibt sich **EAL2+**

## 5.4 Minimale Stärke der Sicherheitsfunktionen des EVGs

149 Die minimale Stärke der durch Wahrscheinlichkeits- oder Permutations-mechanismen (Authentisierungsmechanismus) realisierten EVG-Sicherheitsfunktionen soll **SoF-mittel** erreichen.

# 6 Erklärung

150 Der Erklärungsteil eines Schutzprofils stellt eine Art von Qualitätskontrolle des Schutzprofil-Verfassers dar, in der eine Analyse der bisherigen Kapitel hinsichtlich Vollständigkeit, Angemessenheit und Widerspruchsfreiheit durchgeführt wird.

151 Die Erklärung zeigt, dass das Schutzprofil eine vollständige und zusammengehörige Menge von IT-Sicherheitsanforderungen ist und dass ein konformer EVG die Sicherheitserfordernisse wirksam erfüllen würde.

## 6.1 Erklärung der Sicherheitsziele

152 In der nachfolgenden Tabelle 4 wird die Zielrichtung für die einzelnen Sicherheitsziele aufgezeigt. Für jedes Sicherheitsziel für den EVG und für jedes Sicherheitsziel für die Umgebung wird angegeben, welche Bedrohungen abgewehrt und welche Annahmen berücksichtigt werden sollen.

**Tabelle 4: Zuordnung Sicherheitsziele zu Bedrohungen und Annahmen**

| Sicherheitsziel | Bedrohung | Annahme |
|---|---|---|
| O.logZugriff | T.logZugriff | |
| O.phyZugriff | T.phyZugriff | |
| O.AuthÄndern | T.AuthÄndern | |
| O.Störung | T.Störung | |
| OE.Vertrau.WS | T.logZugriff<br>T.AuthÄndern | A.Vertrau.WS |
| OE.Abwesend | T.logZugriff<br>T.AuthÄndern | A.Abwesend |
| OE.Ausspähen | T.logZugriff<br>T.AuthÄndern | A.Ausspähen |

153 Aus Tabelle 4 ist ersichtlich, dass jede Bedrohung und jede Annahme von mindestens einem Sicherheitsziel adressiert wird und jedes Sicherheitsziel mindestens eine Bedrohung oder eine Annahme adressiert.

154 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.

## 6.2 Abwehr der Bedrohungen durch den EVG

155 Im Folgenden wird gezeigt, dass für jede Bedrohung eine angemessene Begründung vorliegt, dass die zugeordneten Sicherheitsziele geeignet sind, die Bedrohung abzuwehren.

**Tabelle 5: Abdeckung der Bedrohungen durch Sicherheitsziele**

| Bedrohung | Sicherheitsziel für den EVG | Sicherheitsziel für die Umgebung |
|---|---|---|
| T.logZugriff | O.logZugriff | OE.Vertrau.WS<br>OE.Abwesend<br>OE.Ausspähen |
| T.phyZugriff | O.phyZugriff | |
| T.AuthÄndern | O.AuthÄndern | OE.Ausspähen<br>OE.Abwesend<br>OE.Vertrau.WS |
| T.Störung | O.Störung | |

156 Erläuterungen zu den Zuordnungen aus Tabelle 5:

157 **T.logZugriff** Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, greift er auf die vertraulichen Daten des EVGs zu. Den logischen Zugriff erlangt S2 beispielsweise, indem er den EVG an die USB-Schnittstelle eines Computersystems anschließt.

- O.logZugriff adressiert die Kompensation der Bedrohung T.logZugriff direkt durch die Forderung nach einer Zugriffskontrolle, die ausschließlich einem autorisierten Benutzer (S1) Zugriff auf den geschützten Speicherbereich gewährt.
- OE.Abwesend unterstützt zusätzlich die Abwehr der Bedrohung T.logZugriff, indem S1 für den Zeitraum seiner Abwesenheit vom Wirtssystem geeignete Sicherheitsmaßnahmen treffen muss, um den zuvor freigegebenen EVG zu schützen.
- OE.Vertrau.WS unterstützt die Abwehr der Bedrohung T.logZugriff, indem unerlaubte Zugriffe vom Wirtssystem und einem eventuell angeschlossen Netzwerk z.B. durch Schadsoftware ausgeschlossen werden.
- OE.Ausspähen unterstützt die Abwehr der Bedrohung T.logZugriff, indem S1 darauf achten muss, dass sein Authentisierungsmerkmal nicht ausgespäht oder reproduziert werden kann.

158 **T.phyZugriff** Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, greift er über eine physische Attacke auf den Speicher des EVGs zu. Eine physische Attacke könnte z.B. folgendes Szenario sein: Der Speicher des EVGs wird durch S2 entnommen. Nach der Entnahme wird der Speicher in einen anderen USB-Datenträger eingesetzt, über den S2 logisch auf den Speicher zugreift.

O.phyZugriff adressiert die Kompensation der Bedrohung T.phyZugriff direkt, durch die Forderung nach der Verschlüsselung der Daten im geschützten Speicherbereich.

159 **T.AuthÄndern** Unter der Annahme, dass S2 in den Besitz des EVGs gelangt, setzt er ein neues Authentisierungsmerkmal. Infolgedessen werden die Daten für S1 unbrauchbar.

O.AuthÄndern adressiert die Kompensation der Bedrohung T.AuthÄndern direkt, durch die Forderung, das Modifizieren des Authentisierungsmerkmals erst nach vorheriger Authentisierung durch S1 zu ermöglichen.

OE.Ausspähen unterstützt die Abwehr der Bedrohung T.AuthÄndern, indem S1 darauf achten muss, dass sein Authentisierungsmerkmal nicht ausgespäht oder reproduziert werden kann.

OE.Abwesend unterstützt zusätzlich die Abwehr der Bedrohung T.AuthÄndern dahingehend, das S1 für den Zeitraum seiner Abwesenheit vom Wirtssystem, geeignete Sicherheitsmaßnahmen treffen muss, um den zuvor freigegebenen EVG zu schützen.

OE.Vertrau.WS unterstützt zusätzlich die Abwehr der Bedrohung T.AuthÄndern, indem unerlaubte Zugriffe vom Wirtssystem und einem eventuell angeschlossen Netzwerk auf den Authentisierungsmechanismus z.B. durch Schadsoftware ausgeschlossen werden.

160 **T.Störung** Durch eine Störung (z.B. Stromausfall oder Betriebssystemfehler) wird der korrekte Betrieb des EVGs gestört. Als Ergebnis bleiben vertrauliche Daten unverschlüsselt oder das Dateisystem des EVGs wird beschädigt.

161

O.Störung adressiert die Kompensation der Bedrohung T.Störung direkt durch die Forderung, dass der EVG nach einer Störung ( z.B. Stromausfall) wieder einen stabilen und konsistenten Zustand erlangt, ohne dass Daten

unverschlüsselt bleiben oder das Dateisystem beschädigt wird.

## 6.3 Berücksichtigung der Annahmen

162 Im Folgenden wird gezeigt, dass für jede Annahme eine angemessene Begründung vorliegt, dass das zugeordnete Sicherheitsziel für die Umgebung geeignet ist, die Annahme abzudecken.

**Tabelle 6: Abdeckung der Annahmen durch Sicherheitsziele**

| Nr. | Annahme | Sicherheitsziel |
|---|---|---|
| 1 | A.Ausspähen | OE.Ausspähen |
| 2 | A.Vertrau.WS | OE.Vertrau.WS |
| 3 | A.Abwesend | OE.Abwesend |

163 Erläuterungen zu den Zuordnungen aus Tabelle 6:

164 **A.Ausspähen** S1 achtet darauf, dass sein Authentisierungsmerkmal nicht ausgespäht werden kann. Das betrifft z.B. das Mitlesen des Passworts oder die Reproduktion des biometrischen Authentisierungsmerkmals.

OE.Ausspähen bildet die Zielvorgabe, die unmittelbar die Annahme umsetzt. Die Annahme ist notwendig, da der EVG nicht erkennen kann, dass es sich um ein reproduziertes Authentisierungsmerkmal handelt.

165 **A.Vertrau.WS** Nach Freigabe des geschützten Speicherbereichs durch S1, erfolgen vom Wirtssystem und einem eventuell angeschlossen Netzwerk keine unerlaubten Zugriffe auf den EVG.

OE.Vertrau.WS bildet die Zielvorgabe, die unmittelbar die Annahme umsetzt. Die Annahme ist notwendig, da der EVG nach der Freigabe die Zugriffe vom Wirtssystem auf den geschützten Speicherbereich nicht kontrollieren kann.

166 **A.Abwesend** Verlässt S1 das Wirtssystem, an das der zuvor freigegebene EVG angeschlossen ist, so trifft er geeignete Maßnahmen um die Daten in seiner Abwesenheit zu schützen. Geeignete Maßnahmen können z.B. eine Arbeitsplatzsperrung über das Betriebssystem oder die Mitnahme des EVGs sein.

OE.Abwesend bildet die Zielvorgabe, die unmittelbar die Annahme umsetzt. Die Annahme ist notwendig, da der EVG

nach Freigabe des geschützten Speicherbereichs nicht kontrollieren kann ob S1 oder S2 auf die Daten zugreift.

## 6.4 Erklärung der funktionalen Sicherheitsanforderungen des EVGs

### 6.4.1 Erklärung der funktionalen Sicherheitsanforderungen des EVGs

167 Für jede funktionale Sicherheitsanforderung des Schutzprofils wird in der folgenden Tabelle 7 und den dazu gehörenden Erläuterungen verdeutlicht, wie die ausgewählte funktionale Komponente einem Sicherheitsziel des EVGs zugeordnet ist und zur Erreichung dieses Sicherheitsziels beiträgt.

**Tabelle 7: Zusammenhang zwischen funktionalen Sicherheitsanforderungen und Sicherheitszielen des EVGs**

| Nr. | Komponente | Name | Sicherheitsziel |
|---|---|---|---|
| 1 | FCS_CKM.1 | Kryptographische Schlüsselgenerierung | O.phyZugriff |
| 2 | FCS_CKM.4 | Zerstörung des kryptographischen Schlüssels | O.phyZugriff |
| 3 | FCS_COP.1 | Kryptographischer Betrieb | O.phyZugriff |
| 4 | FIA_UAU.1 | Zeitpunkt der Authentisierung | O.logZugriff, O.AuthÄndern, |
| 5 | FIA_UAU.6 | Wiederauthentisierung | O.logZugriff, O.AuthÄndern |
| 6 | FIA_SOS.1 | Spezifikation der Geheimnisse | O.logZugriff, O.AuthÄndern |
| 7 | FDP_ACC.1 | Teilweise Zugriffskontrolle | O.logZugriff, O.AuthÄndern |
| 8 | FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen | O.logZugriff, O.AuthÄndern |
| 9 | FMT_SMF.1 | Spezifikation der Management Funktionen | O.AuthÄndern |
| 10 | FMT_SMR.1 | Sicherheitsrollen | O.logZugriff, O.AuthÄndern |
| 11 | FMT_MSA.1 | Management der Sicherheitsattribute | O.AuthÄndern |
| 12 | FPT_FLS.1 | Erhaltung des sicheren Zustandes bei Fehlern | O.Störung |
| 13 | FPT_RCV.4 | Funktionelle Wiederherstellung | O.Störung |

168 Zu 1,2 und 3.: Die Komponenten **FCS_CKM.1**, **FCS_CKM.4** und **FCS_COP.1** sind zur Verschlüsselung der Daten im geschützten Speicherbereich notwendig und dienen somit dem Sicherheitsziel **O.phyZugriff**. In den Sicherheitsvorgaben (Security Target – ST) muss innerhalb der genannten

Komponenten das kryptographische Verfahren und dessen Schlüssellänge definiert werden.

169 Zu 4: Die Komponente **FIA_UAU.1**, die eine Benutzerauthentisierung vor jeglicher anderen TSF-vermittelten Aktion außerdem Zugriff auf den öffentlichen Speicherbereich fordert, ist auf das Sicherheitsziel **O.logZugriff** ausgerichtet, das die Kontrolle des logischen Zugangs zum EVG formuliert. Auch das Ziel **O.AuthÄndern** ist nur durch eine vorherige Authentisierung möglich.

170 Zu 5: Die Komponente **FIA_UAU.6**, die eine Wiederauthentisierung nach jeglicher Verbindungsstörung fordert, dient den Sicherheitszielen **O.logZugriff** und **O.AuthÄndern**. Über eine Verbindungsstörung kann nicht der Sicherheitsmechanismus Zugriffskontrolle umgangen werden.

171 Zu 6: Die Komponente **FIA_SOS.1** fordert einen Authentisierungsmechanismus der sicherstellt, dass das Authentisierungssmerkmal die Forderung SOF-Mittel erfüllt. Das entsprechend starke Authentisierungsmerkmal dient den Sicherheitszielen **O.logZugriff** und **O.AuthÄndern**.

172 Zu 7: Die Komponente **FDP_ACC.1** fordert eine teilweise Zugriffskontrolle und dient damit dem Sicherheitsziel **O.logZugriff und O.AuthÄndern**, indem ein kontrollierter Zugriff von S1 auf die Ressourcen des EVGs, außer dem öffentlichen Speicherbereich gefordert wird.

173 Zu 8: Die Komponente **FDP_ACF.1** fordert bestimmte Regeln für die benutzerbestimmte Zugriffskontrolle und dient damit den Sicherheitszielen **O.logZugriff** und **O.AuthÄndern**, indem ein kontrollierter Zugriff von Benutzern auf die Ressourcen und Funktion des EVGs formuliert ist, für den implizit bestimmte Regeln gelten müssen.

174 Zu 9: Die Komponente **FMT_SMF.1** fordert eine Funktion zum Modifizieren des Authentisierungsmerkmals und richtet sich somit an das Sicherheitsziel **O.AuthÄndern**.

175 Zu 10: Die Komponente **FMT_SMR.1** fordert die Rolle autorisierter Benutzer (S1). Dies ist erforderlich für Verwendung von Authentisierungsdaten der benutzerbestimmten Zugriffskontrolle (siehe **FDP_ACF.1** und **FDP_ACC.1**). Damit unterstützt die Komponente die Sicherheitsziele **O.logZugriff** und **O.AuthÄndern**.

176 Zu 11: Die Komponente **FMT_MSA.1** fordert, dass das Management des Authentisierungsmerkmals nur für durch den autorisierten Benutzer (S1) möglich ist. Damit dient die Komponente dem Sicherheitsziel **O.AuthÄndern**.

177 Zu 12: Die Komponente **FPT_FLS.1** fordert, dass die TSF bei Auftreten einer Störung (z.B. Stromausfall) einen sicheren Zustand erhalten. Damit dient die Komponente dem Sicherheitsziel **O.Störung**.

178 Zu 13.: Die Komponente **FPT_RCV.4** fordert, dass die TSF sicherstellen, dass nach einer Störung (z.B. Stromausfall) die Sicherheitsfunktion entweder erfolgreich abgeschlossen wird oder diese bis zu einem konsistenten und

sicheren Zustand wiederhergestellt wird. Damit dient die Komponente dem Sicherheitsziel **O.Störung**.

### 6.4.2 Zuordnung: Funktionale Sicherheitskomponenten zu Sicherheitszielen

179 Die folgende **Tabelle 8** zeigt, dass für jedes genannte Sicherheitsziel des EVGs mindestens eine funktionale Sicherheitskomponente aus Teil 2 der CC [CC-Teil2] ausgewählt wurde, welche das jeweilige Sicherheitsziel unterstützt.

**Tabelle 8: Abdeckung Sicherheitsziele durch funktionale Komponenten**

| Sicherheitsziel | Ausgewählte Komponente |
|---|---|
| O.logZugriff | FIA_UAU.1, FIA_UAU.6, FIA_SOS.1,<br>FDP_ACC.1, FDP_ACF.1,<br>FMT_SMR.1 |
| O.phyZugriff | FCS_CKM.1, FCS_CKM.4, FCS_COP.1 |
| O.AuthÄndern | FIA_UAU.1, FIA_UAU.6, FIA_SOS.1,<br>FDP_ACC.1,FDP_ACF.1,<br>FMT_SMF.1, FMT_SMR.1 |
| | FMT_MSA.1 |
| O.Störung | FPT_FLS.1, FPT_RCV.4 |

180 Das Ziel, den Zugang zu den vertraulichen Daten des EVGs über eine Zugriffskontrolle auf autorisierte Benutzer zu beschränken (**O.logZugriff**), wird durch Forderungen nach Authentisierung des Benutzers vor jeglicher anderen Aktion außer dem Zugriff auf den öffentlichen Speicherbereich (FIA_UAU.1) und Wiederauthentisierung bei einer Verbindungsstörung (FIA_UAU.6) erreicht. Die TSF müssen die Rolle autorisierter Benutzer (S1) enthalten, dies wird über (FMT_SMR.1) realisiert. Welche Operationen einem Benutzer abhängig von der Authentisierung gewährt werden, bestimmen die Komponenten (FDP_ACC.1,FDP_ACF.1). Um den logischen Zugang zu schützen muss ein entsprechend starkes Authentisierungsmerkmal gewählt werden (FIA_SOS.1).

181 Das Ziel, den Speicher bei einer physischen Attacke durch Verschlüsselung zu schützen (**O.phyZugriff**) wird durch die Komponenten (FCS_CKM.1, FCS_CKM.4 und FCS_COP.1) realisiert, die den Ablauf der Ver-/Entschlüsselung der Daten bestimmen.

182 Das Ziel, den EVG vor Missbrauch der Funktion zum Modifizieren des Authentisierungsmerkmals durch eine erforderliche Authentisierung von S1 zu schützten (**O.AuthÄndern**) wird in erster Linie von der Komponente

(FMT_MSA.1) bestimmt. Diese Forderung ist abhängig von der Realisierung des Authentisierungsmechanismus (FIA_UAU.1, FIA_UAU.6) und der teilweisen Zugriffskontrolle (FDP_ACC.1,FDP_ACF.1 und FMT_SMR.1). Um die Funktion zur Modifikation des Authentisierungsmerkmal zu schützen muss ein entsprechend starkes Authentisierungsmerkmal gewählt werden (FIA_SOS.1).

183

184 Das Ziel, den EVG vor Missbrauch der Funktion Modifizieren des Authentisierungsmerkmals durch eine erforderliche Authentisierung von S1 zu schützten (**O.AuthÄndern**) fordert das Vorhandensein einer Funktion zum Modifizieren des Authentisierungsmerkmals (FMT_SMF.1). Ziel ist es die Nutzung dieser Funktion auf S1 zu beschränken (FMT_MSA.1). Dies ist abhängig von der Realisierung des Authentisierungsmechanismus (FIA_UAU.1, FIA_UAU.6) und der teilweisen Zugriffskontrolle (FDP_ACC.1,FDP_ACF.1 und FMT_SMR.1).

185

186 Das Ziel, dass der EVG im Falle einer Störung wieder einen konsistenten und stabilen Zustand erlangt und keine Daten durch die Störung unverschlüsselt bleiben oder das Dateisystem beschädigt wird (**O.Störung**), realisieren die Komponenten (FPT_FLS.1, FPT_RCV.4).

## 6.5 Erklärung der Sicherheitsanforderungen an die Umgebung

### 6.5.1 Zuordnung Sicherheitsanforderungen an die Umgebung zu den Sicherheitszielen für die IT-Umgebung

| Nr. | Name | Sicherheitsziel für die IT-Umgebung |
|---|---|---|
| 1 | RE.Vertrau.WS | OE.Vertrau.WS |
| 2 | RE.Abwesend | OE.Abwesend |

187 Zu 1: Die Komponente RE.Vertrau.WS fordert, dass das Wirtssystem die Eigenschaft besitzt unerlaubte Zugriffe über das Wirtssystem (z.B. durch Schadsoftware) oder ein angeschlossenes Netzwerk zu verhindern. Somit dient diese Sicherheitsanforderung dem Sicherheitsziel OE.Vertrau.WS indem keine unerlaubten Zugriffe vom Wirtssystem oder einem angeschlossenen Netzwerk auf den EVG ausgehen.

188 Zu 2: Die Komponente RE.Abwesend fordert, dass das Wirtssystem die Eigenschaft besitzt, es S1 zu ermöglichen den logischen Zugang zum EVG zu blockieren oder zu trennen. Somit dient diese Sicherheitsanforderung dem Sicherheitsziel OE.Abwesend, da S1 für den Zeitraum seiner Abwesenheit den logischen Zugang zum EVG blockieren oder trennen kann.

## 6.6 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVGs

189 Die Anforderungen an die Vertrauenswürdigkeit gemäß der gewählten Vertrauenswürdigkeitsstufe **EAL 2+** sind angemessen für den EVG, weil somit das Ziel eine Basissicherheitsleistung zu gewährleisten erreicht werden soll. Die Sicherheitsleistung des EVGs soll vor logischen und physischen Angriffen schützen.

190

191 Nach den CC bedeutet EAL 2: strukturell getestet

192 EAL2 schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen und Schnittstellenspezifikation sowie von Handbüchern und des Entwurfs des EVGs (TOE) auf hoher Ebene analysiert werden, um das Sicherheitsverhalten zu verstehen.

193 Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse, durch Analyse der Stärke der Funktionen und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen (zum Beispiel solchen die allgemein bekannt sind).

194 EAL2 schafft Vertrauenswürdigkeit auch mittels eines Konfigurationsverzeichnisses für den EVG (TOE) und durch einen Nachweis der Sicherheit der Auslieferungsprozeduren.

195 In diesem Schutzprofil wurde EAL2 um die Komponente **ADV_SPM.1** erweitert, daraus resultiert EAL2+. Diese Komponente fordert vom Entwickler den Nachweis, dass die TSF eine definierte Sicherheitspolitik durchsetzen. Die Erweiterung ist notwendig zur Erfüllung des Sicherheitsziels O.Störung.

196 Die geforderte Mindeststärke der Funktionen der Stufe **SoF-mittel** wurde gewählt, weil die Sicherheitsfunktionen des EVGs die auf dem Authentisierungsmechanismus basieren (umgesetzt durch FIA_SOS.1 und FIA_UAU.1) in der Lage sein sollen, einem moderaten Angriffpotenzial standzuhalten und damit einen angemessenen Schutz vor einfachen, absichtlichen und direkten Attacken durch den Angreifer bieten.

197 Es ist davon auszugehen, dass beim Angreifer Interesse besteht Kenntnis von den wertvollen Daten im Speicher zu nehmen (Beispiele für mögliche wertvolle Daten, siehe Kapitel 2.5). Des Weiteren sind physische Angriffe auf den EVG möglich. Der Angreifer verfügt über die Möglichkeit sich einen zum EVG baugleichen USB-Datenträger zu verschaffen. An diesem USB-Datenträger kann er sowohl logische als auch physische Angriffe erproben. Durch die kompakte Bauweise des EVGs sollte es einem Angreifer relativ einfach möglich sein, den EVG in seinen Besitz zu bringen. Daher verfügt der

EVG über Sicherheitsfunktion, um die vertraulichen Daten sowohl vor logischen als auch vor physischen Angriffen zu schützen.

198 Somit ist die SoF-Forderung konform zu den Bedrohungen und Sicherheitszielen des EVGs und seiner Einsatzumgebung.

## 6.7 Abschließende Erklärung zu den IT-Anforderungen

199 Die im Erklärungsteil beschriebenen Ausführungen zu den Sicherheitszielen haben gezeigt, dass die Summe der IT-Sicherheitsanforderungen geeignet ist, alle Sicherheitsziele des EVGs abzudecken. Keine der beschriebenen IT-Sicherheitsanforderungen steht im Gegensatz zu anderen IT-Sicherheitsanforderungen.

200 Die Summe der IT-Sicherheitsanforderungen bildet ein sich gegenseitig unterstüzendes und in sich konsistentes Ganzes.

# 7 Referenzen

[CC-Teil2] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 2: Funktionale Sicherheitsanforderungen“, Version 2.1, August 1999.

[CC-Teil3] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 3: Anforderungen an die Vertrauenswürdigkeit“, Version 2.1, August 1999.