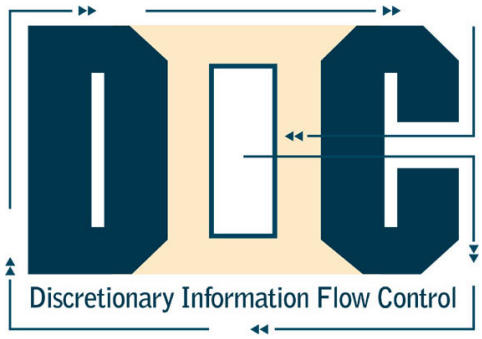
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

Sichere Software

Common Criteria Schutzprofil

Benutzerbestimmbare Informationsflusskontrolle (MU)



Zertifizierungs-ID	BSI-PP-0008
Identifikator	01345-BISS-MU
Versions-Nr.	2.01
Erstellungsdatum	4. September 2002
Verfasser	Dr. Steffen Lange Dr. Andreas Nonnengart Christian Stüble Roland Vogt

Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI GmbH),
Transferzentrum Sichere Software, Stuhlsatzenhausweg 3, 66123 Saarbrücken

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 PP–Einführung

1.1 PP–Identifikation

Titel: Benutzerbestimmbare Informationsflusskontrolle (MU)

Version: 2.01

Registrierung: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Zertifizierungskennung: BSI-PP-0008

Dieses Schutzprofil steht hierarchisch oberhalb des Schutzprofils „Benutzerbestimmbare Informationsflusskontrolle (SU)“, Zertifizierungskennung BSI-PP-0007 [BISS-SU].

Dieses Schutzprofil wurde erstellt auf der Grundlage von:

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 1-3, Version 2.1, August 1999
- Common Evaluation Methodology for Information Technology Security
  - Part 1, Version 0.6, 11.01.1997
  - Part 2, Version 1.0, August 1999
- CCIMB Final Interpretations, Issue 15.02.2002
- ISO-Guide for the Production of Protection Profiles and Security Targets, Version 0.9, 04.01.2000
- Anwendungshinweise und Interpretationen zum Schema, AIS32, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

1.2 PP–Übersicht

Der TOE (EVG) hat die Aufgabe, die Informationsflüsse eines IT-Systems für Benutzer transparent zu schützen. Hierzu kontrolliert der TOE (EVG) die Zulässigkeit eines Informationsflusses gemäß definierbarer Informationsflussregeln. Die Sicherheitsleistung unterstützt insbesondere IT-Anwender mit geringer IT-Fachkompetenz in der Durchsetzung des Schutzes von Informationen, die einem Sicherheitsbedarf in Bezug auf die Aspekte Vertraulichkeit, Integrität und/oder Authentizität unterliegen. Die EVG-Sicherheitsleistung stellt eine sinnvolle Ergänzung zu etablierten Sicherheitskonzepten wie etwa Zugriffsschutz, Übertragungsschutz, Firewalls oder Virtual Private Networks dar. Anwendungsmöglichkeiten des TOE (EVG) ergeben sich in den Bereichen

- E-Commerce (Data Warehouses etc.),
- E-Government (Auftragsvergabe, Antragswesen etc.),
- Gesundheitswesen (elektronische Patientenakte etc.) sowie bei
- Tele- und Mediendiensten (Telearbeit etc.).

Jedem einzelnen Informationsfluss kann eine seinem Schutzbedarf entsprechende Kombination von Sicherheitsmechanismen zugeordnet werden. Für die kontrollierten Informationen gewährleisten diese Mechanismen selektiv den Schutz

- der Integrität durch elektronische Signatur,
- der Vertraulichkeit durch Verschlüsselung und
- der Authentizität durch elektronische Zertifikate.

Der Erhalt der Vertraulichkeit dient dabei der Verhinderung unerwünschter Kenntnisnahme von lokal gespeicherten Benutzerdaten (z.B. nach Diebstahl von Datenträgern oder bei zweckfremder Verarbeitung) und von Benutzerdaten während einer Nachrichtenübertragung. Die Integrität und Authentizität ist insbesondere von Bedeutung bei kommerziellen Transaktionen (z.B. bei elektronischen Bestell- und Bezahlvorgängen).

Ein weiterer Schutzmechanismus besteht in der Einschränkung der Verarbeitung von Informationen auf bestimmte Subjekte (bspw. Applikationen). Damit kann in einem technischen Sinne eine Realisierung der Zweckbindung der Informationsverarbeitung in Übereinstimmung mit Datenschutzbestimmungen unterstützt werden.

Der TOE (EVG) arbeitet weitestgehend transparent für die betroffenen Subjekte (bspw. Applikationen) und für die Benutzer des IT-Systems. Eine Anpassung der auf dem IT-System eingesetzten Applikationen ist nur insoweit erforderlich, als dem TOE (EVG) die für die Ausübung der Kontrolle benötigten Angaben über den jeweiligen Informationsfluss zur Verfügung gestellt werden müssen. Flexible Konfigurationsoptionen ermöglichen eine individuelle und fortlaufende Anpassung des TOE (EVG) an den Schutzbedarf des Betreibers des IT-Systems.

Das Schutzprofil abstrahiert die Anforderungen an den TOE (EVG) so weit von technischen Details, dass eine Realisierung für eine Reihe unterschiedlicher IT-Umgebungen möglich ist, wie z.B.

- (Mehrbenutzer-) Betriebssysteme,
- Datenbanksysteme oder
- Email-Clients und -Server.

Die hier beschriebene Sicherheitsleistung verlangt von der IT-Umgebung die Fähigkeit zur Unterscheidung von Benutzern. Falls auf diese Unterscheidung verzichtet werden kann, ist die Verwendung eines TOE (EVG) möglich, der mit der Einbenutzervariante [BISS-SU] des Schutzprofils konform ist.

Der TOE (EVG) kann auf vielfältige Weise in die jeweilige IT-Umgebung eingebunden sein. So kann bspw. ein Service-Prozess eines Betriebssystems (etwa ein Email-Server) sowohl als einzelnes Subjekt verstanden werden, das von einem ins Betriebssystem eingebetteten TOE (EVG) kontrolliert wird, als auch als eigenständige IT-Umgebung für einen TOE (EVG), der die mit dem Server kommunizierenden Clients kontrolliert.

1.3 PP–Organisation

Die wesentlichen Bestandteile des Schutzprofils sind die EVG-Beschreibung, die EVG-Sicherheitsumgebung, die Sicherheitsziele, die IT-Sicherheitsanforderungen und die Erklärung.

Die EVG-Beschreibung liefert allgemeine Informationen über den TOE (EVG), dient als Hilfe zum Verständnis der Sicherheitsanforderungen und liefert Zusammenhänge für die Evaluation des Schutzprofils. Es werden die Art des Produkts und die allgemeinen IT-Leistungsmerkmale des TOE (EVG) beschrieben. In den Abschnitten EVG-Abgrenzung und Betriebsumgebung des TOE (EVG) werden die Bestandteile des TOE (EVG) und seine Einbettung in die Betriebsumgebung aufgezeigt. Zur Erleichterung des Verständnisses der Sicherheitskonzepte des TOE (EVG) werden im Abschnitt EVG-Sicherheitspolitik zunächst deren grundlegenden Begriffe definiert. Daran schließt sich die detaillierte Beschreibung der Sicherheitsprinzipien und -charakteristika der funktionalen Sicherheitspolitik (SFP) der benutzerbestimmbaren Informationsflusskontrolle an.

Die EVG-Sicherheitsumgebung beschreibt Sicherheitsaspekte der Umgebung, in welcher der TOE (EVG) verwendet wird, und die Art und Weise, wie er zu gebrauchen ist. Die EVG-Sicherheitsumgebung beinhaltet Beschreibungen von

a) Annahmen in Bezug auf die Umgebung, in der der TOE (EVG) eingesetzt wird,
b) Bedrohungen, die durch den TOE (EVG) abgewendet werden sollen, und
c) organisatorischen Sicherheitspolitiken, die vom TOE (EVG) durchzusetzen sind.

Die Sicherheitsziele legen (produktunabhängig) den Zweck des Schutzprofils dar. Dazu gehört, wie der TOE (EVG) erkannten Bedrohungen begegnet und wie er ausgewiesene organisatorische Sicherheitspolitiken und Annahmen abdeckt. Für jedes Sicherheitsziel ist festgelegt, ob es für den TOE (EVG) oder die Umgebung gilt.

Das Kapitel IT-Sicherheitsanforderungen stellt, in separaten Teilabschnitten, detaillierte Sicherheitsanforderungen für den TOE (EVG) und seine Umgebung zur Verfügung. Die EVG-Sicherheitsanforderungen sind wie folgt unterteilt:

a) Funktionale Sicherheitsanforderungen an den TOE (EVG), zuzüglich Anforderungen an die Stärke der EVG-Sicherheitsfunktionen, die auf einem Wahrscheinlichkeits- oder Permutationsmechanismus beruhen, und
b) Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

Die Erklärung weist nach, dass das Schutzprofil eine vollständige und zusammengehörige Menge von IT-Sicherheitsanforderungen ist und dass ein konformer TOE (EVG) die Sicherheitserfordernisse wirksam ansprechen würde. Die Erklärung besteht aus zwei Hauptteilen. Zuerst wird anhand einer Erklärung zu den Sicherheitszielen gezeigt, dass die Sicherheitsziele auf alle in der EVG-Sicherheitsumgebung genannten Aspekte zurückgeführt werden können und dass sie geeignet sind diese abzudecken. Dann wird anhand einer Erklärung zu den Sicherheitsanforderungen gezeigt, dass die Sicherheitsanforderungen (für den TOE (EVG) wie auch für die Umgebung) auf die Sicherheitsziele zurückgeführt werden können, und dass sie geeignet sind, diese Ziele zu erreichen.

2 EVG-Beschreibung

Zu diesem Schutzprofil konforme Produkte bestehen im Allgemeinen aus einer oder mehreren Komponenten, welche die bereits existierenden Ein-/Ausgabefunktionen des IT-Systems um eine benutzerbestimmbare Informationsflusskontrolle erweitern. Die Anforderungen an den TOE (EVG) werden so allgemein gehalten, dass die Erstellung konformer Produkte für verschiedene IT-Umgebungen gewährleistet ist. Das Einsatzspektrum des TOE (EVG) umfasst die Bereiche geschützte lokale Datenspeicherung und -verarbeitung sowie geschützte Datenübertragung über offene Netzwerke.

Kontrolliert werden sowohl innerhalb des IT-Systems stattfindende Informationsflüsse, wie z.B. die Speicherung oder das Laden von Dateien, als auch aus dem IT-System herausführende Informationsflüsse, wie z.B. der Versand oder Empfang von Emails. Zur Identifikation von Informationsflüssen werden die Kennungen der auslösenden Benutzer, die verarbeitende funktionale Einheit (z.B. eine Applikation) und der Aufbewahrungsort (z.B. Verzeichnisse, Rechner- oder Emailadressen) verwendet. Eine Plausibilitätskontrolle und Konsistenzprüfung verhindert, dass Informationsflussregeln unzweckmäßig sind oder sich widersprechen. Beides erleichtert auch die Administration des TOE (EVG).

Für den Benutzer ist der TOE (EVG) grundsätzlich unsichtbar. Nur bei Fehlermeldungen, bei der Anwendung von Signatur- und Verschlüsselungsverfahren und im Fall, dass Informationsflüsse explizit zu autorisieren sind, wird der TOE (EVG) wahrgenommen.

2.1 Art des Produkts

Der TOE (EVG) ist ein betriebssystemnaher Teil eines IT-Systems, bzw. ein Bestandteil seines Betriebssystems. Zur Realisierung der TSF ist ein modularer Aufbau zweckmäßig, der die Integration des TOE (EVG) mit unterschiedlichen Anwendungsdiensten wie bspw. Datenbanksystemen und Email-Services ermöglicht. Der TOE (EVG) kann sowohl als reine Softwarelösung als auch als eine kombinierte Lösung aus Software- und Hardware-Komponenten realisiert werden. Insbesondere für die Speicherung und Anwendung von kryptographischen Schlüsseln kann der TOE (EVG) ggf. auf geeignete (Hardware-)Module in der IT-Umgebung zurückgreifen.

2.2 IT-Leistungsmerkmale

Der TOE (EVG) stellt sicher, dass Informationsflüsse sowohl innerhalb des IT-Systems als auch aus dem IT-System hinaus (über eine Verbindung zu offenen Netzen, bspw. LAN, WAN, Internet, Email) in Übereinstimmung mit der zugrunde liegenden EVG-Sicherheitspolitik und gemäß der festgelegten Informationsflussregeln stattfinden. Die Informationsflussregeln können aus vorgegebenen rechtlichen, technischen und organisatorischen Regelungen (z.B. verschlüsselte Speicherung, verschlüsselte Übertragung, signierte Übertragung) abgeleitet werden. In Informationsflussregeln kann festgelegt werden, unter welchen Umständen der TOE (EVG) auf welche Art und Weise mit Da-

ten zu verfahren hat. Die Entscheidung über die Erlaubnis von Informationsflüssen und ihre vorschriftsmäßige Verarbeitung leistet der TOE (EVG) mit Hilfe eines Referenzmonitors, der die Informationsflüsse überwacht.

2.3 EVG-Abgrenzung

Der TOE (EVG) besteht aus einem immer aktiven funktionalen Verarbeitungsteil, bestehend aus Referenzmonitor, Kontroll- und Verarbeitungsfunktionen sowie aus einer Liste von Informationsflussregeln. Der funktionale Verarbeitungsteil überwacht und verarbeitet die Informationsflüsse. Daneben existieren Funktionen zur Konfiguration, Administration und Protokollauswertung.

Anwendungsbemerkung 1. Der ST-Autor hat die Bestandteile des TOE (EVG) näher zu beschreiben, z.B. wenn für die Administration ein eigenständiges Programm vorgesehen ist.

Das vorliegende Schutzprofil ist so formuliert, dass für die Realisierung von Produkten verschiedene Architekturen möglich sind:

- Component TOE (EVG) – Die Funktionen zur Informationsflusskontrolle und zur Speicherung und Anwendung kryptographischer Schlüssel sind voneinander separiert. Dies erlaubt insbesondere die Verwendung von vorgefertigten Krypto-Modulen.
- Composite TOE (EVG) – Die Funktionen zur Informationsflusskontrolle und zur Speicherung und Anwendung kryptographischer Schlüssel sind integrale Bestandteile des Produkts.

Die IT-Sicherheitsanforderungen sind so spezifiziert, dass das Schutzprofil für die Realisierung eines Component TOE (EVG), der für den kryptographischen Betrieb auf externe Dienste zurückgreift, unmittelbar geeignet ist. Für die Konformität eines Composite TOE (EVG), der diese Funktionalität als integralen Bestandteil enthält, sind die erforderlichen funktionalen Komponenten zu den EVG-Sicherheitsanforderungen zu verschieben. Dies betrifft insbesondere die Komponente FCS_COP.1, die dann Anforderungen an den TOE (EVG) und nicht an seine IT-Umgebung stellt.

Eine mögliche Struktur des TOE (EVG) und seine Einbettung in die IT-Umgebung ist in Abbildung 1 als Blockdiagramm dargestellt. Der TOE (EVG) besteht hierbei aus dem unterlegten Bereich. Das Basismodul stellt die Grundfunktionalität (Referenzmonitor) bereit. Die Erweiterungsmodule binden unterschiedliche Anwendungsdienste (bspw. Datenbanksysteme und Email-Services) sowie die Funktionen zur Konfiguration, Administration und Protokollauswertung an.

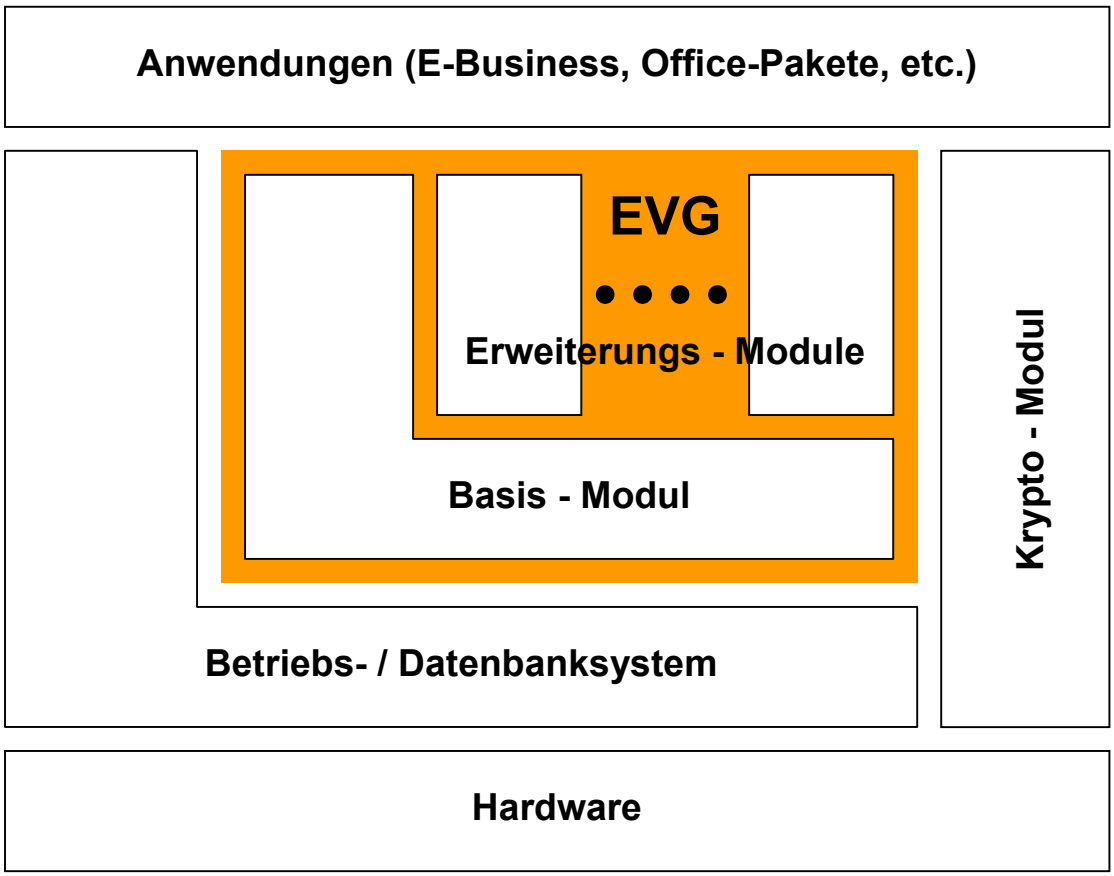


Abbildung 1: Mögliche Struktur des TOE (EVG) in der IT-Umgebung

2.4 Betriebsumgebung

Es wird angenommen, dass nicht jeder rechtmäßige Benutzer ein Interesse an der Sicherheitsleistung des TOE (EVG) hat und direkte Bedrohungen von Benutzerdaten durch andere rechtmäßige Benutzer ausgehen. Um unerwünschte Informationsflüsse, die von rechtmäßigen Benutzern angefordert werden, verhindern zu können, ist eine Unterscheidung der Benutzer notwendig. Es wird angenommen, dass der TOE (EVG) in einer Umgebung betrieben wird, in der Benutzer unterschieden werden.
Darüber hinaus muss auch von Administratoren des IT-Systems (insbesondere im Fall einer Fernadministration) ein fehlendes Interesse an der Sicherheitsleistung des TOE (EVG) angenommen werden. Sie werden ebenso wie nicht rechtmäßige Benutzer (potentielle Angreifer) als Urheber von Bedrohungen betrachtet. Es wird von einem Angriffspotential ausgegangen, das auf die Fähigkeit zur Durchführung offensichtlicher Penetrationsangriffe beschränkt ist.
Eine Sonderstellung nimmt der EVG-Administrator ein. Er wird ohne Einschränkung als vertrauenswürdig angesehen. Maßnahmen zur Kontrolle der Tätigkeit des EVG-Administrators sind daher nicht vorgesehen.

2.5 EVG-Sicherheitspolitik

Dieses Kapitel erläutert die vom TOE (EVG) durchzusetzende EVG-Sicherheitspolitik, die *Funktionale Sicherheitspolitik (SFP) der benutzerbestimmbaren Informationsflusskontrolle*. Zur Beschreibung der Sicherheitspolitik wird zwischen aktiven Einheiten (den Subjekten), passiven Einheiten (den Objekten) und den Informationen unterschieden. Objekte können Informationen enthalten und sind Ziel von Operationen, die von Subjekten ausgeführt werden. Subjekten, Objekten und Informationen werden Sicherheitsattribute zugeordnet, die die Grundlage für die Politikentscheidungen der SFP der benutzerbestimmbaren Informationsflusskontrolle bilden.

2.5.1 Begriffsbestimmung

Unter einem **Informationsfluss** wird die Ein-/Ausgabe einer IT-Komponente von/zu einem beliebigen Datenort verstanden. Er ist durch die Angabe eines Subjekts, eines Objekts und einer Operation gekennzeichnet.

Ein Informationsfluss wird von einem **Subjekt** ausgelöst. Dieses wird identifiziert durch eine Benutzerkennung und eine aktive funktionale Einheit, bspw. eine Applikation (ein Anwendungsprogramm, dem Prozesse auf Betriebssystemebene zugeordnet werden können).

Die von/zu Subjekten fließende Information bildet zusammen mit dem Behälter, in dem sie aufbewahrt wird, das kontrollierte **Objekt**. Der Behälter ist typischerweise eine Datei, kann aber auch bspw. als ein Datensatz in einem Datenbanksystem oder als das einer Email-Adresse zugeordnete Postfach verstanden werden.

Der **Datenort** beschreibt die Stelle, an der ein Objekt aufbewahrt wird. Ein Datenort bezieht sich bspw. auf ein lokales Speichermedium, einen über eine Netzwerkverbindung erreichbaren Adressaten oder eine Rechneradresse. Für ein Speichermedium kann ein Datenort aus einer Pfadinformation bezüglich einer Verzeichnishierarchie bestehen. Für Netzverbindungen typisch ist die Angabe einer Email-Adresse.

Zur gegenseitigen Abgrenzung der Begriffe Information, Objekt und Datenort sei ein illustrierendes Beispiel außerhalb der Informationstechnologie gewählt: Der traditionelle Briefpostverkehr. Die Information entspricht hier dem Inhalt eines Briefes. Dieser bildet zusammen mit dem Briefumschlag (also dem Behälter) das Objekt. Das Postfach, in dem der Brief aufbewahrt wird, entspricht dem Datenort.

Schließlich werden zwei Operationen definiert:

read(S; I; O)	Subjekt S liest eine Information I aus einem Objekt O.
write(S; I; O)	Subjekt S schreibt eine Information I in ein Objekt O. Eine bereits in O enthaltene Information wird dabei ggf. gelöscht.

Anwendungsbemerkung 2. In vielen Fällen besteht eine Lese-/Schreiboperation aus mehreren Operationen, bspw. kann ein vorheriges Öffnen und nachträgliches Schließen einer Datei nötig sein. In der SFP der benutzerbestimmbaren Informationsflusskontrolle wird eine Lese-/Schreiboperation als eine nicht unterbrechbare (atomare) Operation betrachtet. Dies ist notwendig, um Konflikte bei Änderungen von Informationsflussregeln zu vermeiden. Damit wird also von den konkreten Gegebenheiten in der IT-Umgebung abstrahiert. Folglich muss der Hersteller eines zu diesem Schutzprofil konformen Produktes dafür sorgen, dass die Atomarität der beiden Operationen read(…) und write(…) eingehalten wird.

Eine **Informationsflussregel** besteht aus den folgenden Angaben:

- einer Operation
- einer Menge von Subjekten
- einer Menge von Datenorten
- einem Kontrollflag (Bez. CF)
- einem Vertrauenswürdigkeitsflag (Bez. TF)
- einem Protokollierungsflag (Bez. PF)
- einer Menge von Informationsflussvorschriften.

Mögliche Operationen sind Lesen (read) und Schreiben (write) von Information.
Ein Informationsfluss mit kontrollierten Objekten wird nur erlaubt, wenn das anfordernde Subjekt in der Menge der Subjekte genannt ist. Damit können die zur zweckgebundenen Verarbeitung der Information zugelassenen Subjekte bestimmt werden. Um Mengen von Subjekten kompakt beschreiben zu können, ist die Verwendung von Platzhaltern (Wildcards) erlaubt.
Sämtliche Informationsflüsse mit allen an den genannten Datenorten aufbewahrten bzw. neu erzeugten Objekten werden in Übereinstimmung mit den Informationsflussvorschriften durchgeführt. Um Mengen von Datenorten kompakt beschreiben zu können, ist die Verwendung von Platzhaltern (Wildcards) erlaubt.
Das Kontrollflag CF wird „True“ gesetzt, um zum Ausdruck zu bringen, dass mit den genannten Datenorten nur Informationsflüsse gemäß vorhandener Informationsflussregeln stattfinden dürfen. Damit kann das wesentliche Merkmal von Informationsflusskontrolle gewährleistet werden, nämlich dass zu kontrollierende Information im kontrollierten Bereich verbleibt.
Das Vertrauenswürdigkeitsflag TF wird „True“ gesetzt, wenn es den genannten Subjekten gestattet ist, die an den genannten Datenorten befindliche Information ohne Aufrechterhaltung des Schutzes an andere Datenorte zu schreiben. Damit ist es möglich, Ausnahmen zur o.g. Abgrenzung des kontrollierten Bereichs zu spezifizieren.
Das Protokollierungsflag PF wird „True“ gesetzt, wenn alle Anforderungen von Informationsflüssen, die gemäß dieser Informationsflussregel erlaubt bzw. verweigert werden, zu protokollieren sind.
Über entsprechende Informationsflussvorschriften kann die Authentizität, Integrität bzw. Vertraulichkeit der an den genannten Datenorten aufbewahrten Information geschützt werden. In den Informationsflussvorschriften zum Schreiben von Information muss mindestens festgelegt werden können, dass die Information zu verschlüsseln bzw. zu signieren ist (ggf. mit Hinweis auf zu verwendende Verfahren und Schlüssel zum Verschlüsseln bzw. Signieren). Entsprechend muss in Informationsflussvorschriften zum Lesen von Information mindestens festgelegt werden können, dass die vorliegen-

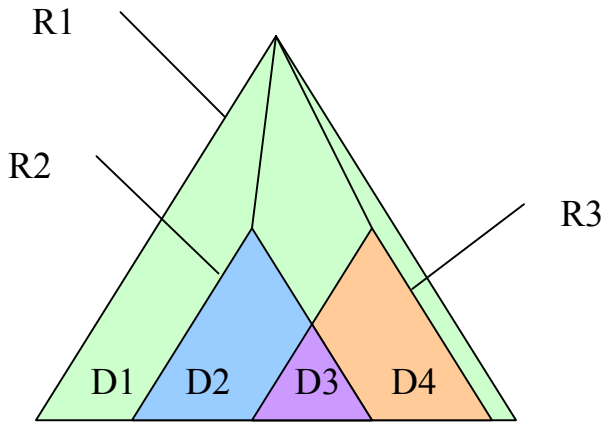
den Daten zu entschlüsseln sind (ggf. mit Hinweis auf zu verwendende Verschlüsselungsverfahren und Schlüssel) bzw. die Gültigkeit von mit den Daten verknüpften Signaturen zu prüfen ist (ggf. mit Hinweis auf zu verwendende Prüfverfahren und Schlüssel).
Darüber hinaus können in Informationsflussvorschriften zum Lesen bzw. Schreiben von Information weitere Funktionen einbezogen werden. Es kann bspw. festgelegt werden, dass es notwendig ist, vor dem Lesen zunächst die vorliegenden Daten zu dekomprimieren (ggf. mit Hinweis auf das zu verwendende Komprimierungsprogramm) oder auf Virenfreiheit zu testen (ggf. mit Hinweis auf das zu verwendende Virenschutzprogramm) bzw. vor dem Schreiben die Daten zu komprimieren (ggf. mit Hinweis auf das zu verwendende Komprimierungsprogramm).

Um unterschiedlichen Sicherheitsbedürfnissen gerecht zu werden, können Informationsflussregeln in einer **Liste von Informationsflussregeln** zusammengefasst werden.

Es seien also eine Liste von Informationsflussregeln und ein Datenort D gegeben. Eine Informationsflussregel R ist eine **spezifischste Informationsflussregel für D**, falls D in der Informationsflussregel R genannt ist und es in der Liste keine Informationsflussregel R' gibt, in der neben D nur einige der in R genannten Datenorte genannt werden.

Mit Hilfe des Begriffs spezifischste Informationsflussregel ist es möglich, eine Hierarchie unter den Informationsflussregeln aufzubauen und auf diese Weise die Informationsflussregeln zu identifizieren, deren Fokus so eng wie möglich auf den aktuellen Datenort eingegrenzt ist.

Illustration. Wie in Abbildung 2 dargestellt, werden in der Informationsflussregel R1 die Datenorte D1, D2, D3 und D4, in Regel R2 die Orte D2 und D3 sowie in Regel R3 die Orte D3 und D4 genannt. Die Tabelle ordnet den dargestellten Datenorten die jeweils spezifischsten Informationsflussregeln zu. Dabei ist insbesondere zu beachten, dass sich die Mengen der in den Informationsflussregeln R2 und R3 genannten Datenorte überschneiden. Da jeweils der Datenort D3 genannt wird, sind somit sowohl R2 als auch R3 spezifischste Informationsflussregeln für D3.



	D1	D2	D3	D4
R1	✕	—	—	—
R2	—	✕	✕	—
R3	—	—	✕	✕

Abbildung 2: Illustration zum Begriff „spezifischste Informationsflussregel"

Überlappungen verschiedener Informationsflussregeln wie in Abbildung 2 sind insbesondere bei Verwendung von Wildcards für die Bezeichnung von Datenorten sinnvoll, um auf einfache Weise generelle Informationsflussregeln formulieren zu können, zu denen in anderen Regeln Ausnahmen beschrieben sind. Selbstverständlich müssen Konflikte zwischen überlappenden Informationsflussregeln vermieden bzw. aufgelöst werden. Zum einen soll für jeden von einem konkreten Subjekt angeforderten Informationsfluss höchstens eine einzige unter den spezifischsten Regeln zuständig sein. Da je nach anforderndem Subjekt verschiedene Informationsflussregeln zur Anwendung kommen, soll zum anderen die Anwendung dieser Regeln auf das gleiche Objekt nicht zu Datenverlust führen.

Diese Überlegungen legen geeignete Einschränkungen für die Zusammenstellung von Informationsflussregeln nahe. Eine Liste von Informationsflussregeln heißt **konsistent**, falls die folgenden Bedingungen erfüllt sind:

(C1) Wenn die in einer Informationsflussregel formulierte Informationsflussvorschrift Operationen zum Schutz der Vertraulichkeit, Integrität oder Authentizität enthält, so muss das Kontrollflag CF auf den Wert „True“ gesetzt sein.

(C2) Zu jedem Informationsfluss gibt es höchstens eine spezifischste Informationsflussregel, in der das betreffende Subjekt und die aktuelle Operation genannt sind.

(C3) Wenn es für einen Datenort eine spezifischste Informationsflussregel für die Operation Lesen gibt, so gibt es auch eine spezifischste für die Operation Schreiben. Wenn es für einen Datenort eine spezifischste Informationsflussregel für die Operation Schreiben gibt, so gibt es auch eine spezifischste für die Operation Lesen.

(C4) Für je zwei spezifischste Informationsflussregeln für denselben Datenort gilt, dass die in den Informationsflussregeln formulierten Informationsflussvorschriften einander nicht widersprechen.

Der ST-Autor ist verpflichtet zu definieren, was es heißt, dass Informationsflussvorschriften widersprüchlich sind. Diese Definition hat derart präzise zu sein, dass sich daraus ein implementierbares Verfahren ableiten läßt, mit dem festgestellt werden kann, ob Informationsflussvorschriften widersprüchlich sind.

Erläuterung. Wenn bspw. in den Informationsflussvorschriften zweier Informationsflussregeln präzisiert ist, dass unterschiedliche Applikationen unter Verwendung verschiedener Verschlüsselungsverfahren Informationen in das gleiche Objekt schreiben dürfen, widersprechen sich diese Informationsflussvorschriften. Andererseits ist zu beachten, dass bspw. Backup-Verfahren auf jeden Bereich des Speichermediums lesend zugreifen sollen. Das Backup-Verfahren soll die Daten bitweise lesen und bitweise auf das Backup-Medium schreiben (also u.a. ohne vorherige Entschlüsselung). Diese Art der Verarbeitung darf also keiner anderen Informationsflussvorschrift widersprechen.

Für die mittels des TOE (EVG) durchzusetzende SFP der benutzerbestimmbaren Informationsflusskontrolle werden die in Tabelle 1 festgelegten Objekt- und Subjektattribute zugrunde gelegt.

Kategorie	**Attribut**	**mögliche Werte**
Objekt (Bez. O)	Kontrollstatus C(O)	Strong, Weak
Subjekt (Bez. S)	Sicherheitslevel L(S)	High, Low

Tabelle 1: Sicherheitsattribute

Der **Kontrollstatus** eines Objekte dient dazu, die Zweckbindung und den Schutz der Authentizität, Integrität bzw. Vertraulichkeit der in diesem Objekt aufbewahrten Information durchzusetzen. Der Wert „Strong“ gibt an, dass die in dem betreffenden Objekt enthaltenen Informationen zu schützen sind.
Das Sicherheitsattribut C(O) ist unveränderlich und statisch an das Objekt O und damit an die darin befindliche Information gebunden. Es hat den Wert „Strong“, falls sich das Objekt O an einem zu kontrollierenden Datenort D befindet, anderenfalls hat das Sicherheitsattribut C(O) den Wert „Weak“. In diesem Zusammenhang ist ein Datenort D ein **zu kontrollierender** Datenort, falls in einer spezifischsten Informationsflussregel für D das Kontrollflag CF den Wert „True“ hat.

Illustration. Vorausgesetzt sei, dass die Liste der Informationsflussregeln R1 bis R3 aus Abbildung 2 konsistent ist. Es sei nun ein Objekt O betrachtet, das am Datenort D3 aufbewahrt wird. Der Kontrollstatus von O darf nicht davon abhängen, über welche der Regeln R2 und R3 die Informationsflüsse mit O kontrolliert werden. Anderenfalls wäre keine konsistente Durchsetzung einer Sicherheitspolitik für Informationsflusskontrolle möglich. Die Definition des Sicherheitsattributs C(O) legt fest, wie mit unterschiedlichen Angaben in überlappenden Regeln (im betrachteten Beispiel R2 und R3) zu verfahren ist. Wenn bspw. CF(R2) = „True“ und CF(R3) = „False“ gesetzt ist, dann ist, unabhängig davon, ob R2 oder R3 anzuwenden ist, C(O) = „Strong“. Zur Vereinfachung der Administration des TOE (EVG) und zur frühzeitigen Erkennung unerwünschter Effekte sollte im Rahmen der Plausibilitätskontrolle ein Hinweis erfolgen, wenn der Fall eingetreten ist, dass das Kontrollflag in sich überlappenden Informationsflussregeln unterschiedlich gesetzt ist.

Der **Sicherheitslevel** eines Subjektes dient dazu, das wesentliche Merkmal von Informationsflusskontrolle zu gewährleisten, nämlich dass zu kontrollierende Information im kontrollierten Bereich verbleibt. Der Wert „High“ zeigt an, dass das betreffende Subjekt in Besitz von zu schützenden Informationen ist.
Das Sicherheitsattribut L(S) ist veränderlich und variiert zur Laufzeit des Subjekts S. Bei der Generierung eines neuen Subjekts S (bspw. beim Starten einer Applikation), erhält das Sicherheitsattribut L(S) den Wert „Low“ als Anfangswert. Der Wert von L(S) wechselt auf „High“ und behält dann diesen Wert, sobald das Subjekt S Informationen aus einem Objekt O mit Kontrollstatus C(O) = „Strong“ liest. Eine Ausnahme hiervon bilden Informationsflüsse, die als vertrauenswürdig gekennzeichnet sind, d.h. in der zuständigen Informationsflussregel ist TF = „True“ gesetzt.

2.5.2 Sicherheitsprinzipien (Security Principles)

Für die hier beschriebene EVG-Sicherheitspolitik der benutzerbestimmbaren Informationsflusskontrolle werden folgende Sicherheitsprinzipien (security principles) definiert:

(P1) **Protokollierung.** Entscheidungen über die Erlaubnis bzw. Verweigerung von Informationsflüssen werden protokolliert, wenn dies gemäß der Informationsflussregeln erforderlich ist.

(P2) **Datensicherheit.** Erlaubte Informationsflüsse finden immer in Übereinstimmung mit den in den Informationsflussregeln genannten Informationsflussvorschriften statt.

(P3) **Zweckbindung.** Ist der Kontrollstatus eines Objektes O „Strong“, so werden die das Objekt O betreffenden Informationsflüsse nur erlaubt, falls sie von einem Subjekt S angefordert werden, welches hierzu gemäß der Informationsflussregeln autorisiert ist.

(P4) **Informationsflusskontrolle.** Ist der Kontrollstatus eines Objektes O „Strong“ (C(O) = „Strong“), so kann eine Information I, die vom Objekt O stammt, nicht in ein Objekt O' mit C(O') = „Weak“ gelangen, es sei denn, das diesen Informationsfluss auslösende Subjekt S ist gemäß der Informationsflussregeln dazu autorisiert.

(P5) **Benutzerbestimmbarkeit.** Als Ausnahme zu Prinzip (P4 – Informationsflusskontrolle) kann mindestens der EVG-Administrator den Informationsfluss explizit autorisieren, d.h. eine Information I, die von einem Objekt O mit C(O) = „Strong“ stammt, kann dann in ein Objekt O' mit C(O') = „Weak“ gelangen.

Erläuterung. Das Prinzip (P4 – Informationsflusskontrolle) kann nicht ausschließlich unter Verwendung des Sicherheitsattributs Kontrollstatus umgesetzt werden, da die Entscheidung, ob ein schreibender Informationsfluss in Objekt O' zu erlauben ist, davon abhängt, ob die Information I aus einem Objekt O mit C(O) = „Strong“ stammt. Dazu wird der Sicherheitslevel des Subjekts S verwendet. Bei einem lesenden Informationsfluss wird L(S) auf „High“ gesetzt, wenn C(O) = „Strong“ gilt, es sei denn, das Subjekt S ist gemäß der Informationsflussregel als vertrauenswürdig gekennzeichnet, d.h. das Vertrauenswürdigkeitsflag TF hat den Wert „True“.

Anwendungsbemerkung 3. Der ST-Autor kann festlegen, welche Benutzer zusätzlich zum EVG-Administrator Autorisierungen gemäß Prinzip (P5 – Benutzerbestimmbarkeit) vornehmen dürfen. Er hat in einem solchen Fall zu präzisieren, auf welche Weise diese Benutzer die hierfür erforderliche Berechtigung erhalten. Dies kann bspw. mit Hilfe von Besitzrechten erfolgen.

2.5.3 Sicherheitscharakteristika (Security Characteristics)

Im Folgenden werden die der SFP der benutzerbestimmbaren Informationsflusskontrolle zugrunde liegenden Sicherheitscharakteristika (security characteristics) detailliert beschrieben.

Es sei eine konsistente Liste von Informationsflussregeln präzisiert. Um die Entscheidung zu treffen, ob ein angeforderter Informationsfluss erlaubt oder verweigert wird, ist zunächst zu prüfen, ob der zum angeforderten Informationsfluss gehörende Datenort in einer Informationsflussregel genannt ist. Ist das nicht der Fall, kommen die Regeln (CR1) bzw. (CW1) zur Anwendung. Andernfalls muss als nächstes festgestellt werden, welche der vorhandenen Informationsflussregeln zum Treffen dieser Entscheidung heranzuziehen ist, bevor gemäß (CR2) oder (CR3) bzw. (CW2) oder (CW3) verfahren wird. Ist in der heranzuziehenden Informationsflussregel das Protokollierungsflag PF auf „True“ gesetzt, wird die Entscheidung protokolliert (vgl. Prinzip (P1 – Protokollierung)).

Eine **Auswahlfunktion**, die ein wesentlicher Parameter der SFP der benutzerbestimmbaren Informationsflusskontrolle ist, bestimmt die heranzuziehende Informationsflussregel.

Es seien read(S; I; O) bzw. write(S; I; O) der angeforderte Informationsfluss und D der Datenort, an dem das Objekt O aufbewahrt wird. Wenn der Datenort D in wenigstens einer Informationsflussregel genannt ist, wählt die Auswahlfunktion eine Informationsflussregel aus. Die ausgewählte Informationsflussregel R hat die folgenden Eigenschaften:

(S1) R ist eine spezifischste Informationsflussregel für den Datenort D, in der die aktuelle Operation genannt ist.[1]

(S2) Falls es in der Liste der Informationsflussregeln eine spezifischste Informationsflussregel für den Datenort D gibt, in der neben der aktuellen Operation auch das Subjekt S genannt wird, so wird das Subjekt S auch in R genannt.

[1] Die im Abschnitt Begriffsbestimmung formulierten Konsistenzbedingungen stellen sicher, dass es in einer konsistenten Liste von Informationsflussregeln zu jedem in einer Informationsflussregel genannten Datenort eine spezifischste Informationsflussregel gibt, in der die aktuelle Operation genannt ist.

Die SFP der benutzerbestimmbaren Informationsflusskontrolle stützt sich auf die in Tabelle 2 zusammengefassten und nachfolgend beschriebenen Regeln.

Legende *erlaubt/verweigert*: Entscheidung der SFP (C…): Security Characteristics (P…): Security Principles		Auswahlfunktion liefert keine Regel	Auswahlfunktion liefert Regel R		
			Objekt O hat Kontrollstatus C(O) = „Weak“	Objekt O hat Kontrollstatus C(O) = „Strong“	
				Subjekt S wird in Regel R genannt	Subjekt S wird in Regel R nicht genannt
read(S; I; O)		***erlaubt*** (CR1)	***erlaubt*** (CR2) (P1), (P2)	***erlaubt*** (CR3 (i)) (P1), (P2), (P3)	***verweigert*** (CR3 (ii)) (P1), (P3)
write(S; I; O)	L(S) = „Low“	***erlaubt*** (CW1 (i)) (P4)	***erlaubt*** (CW2 (i)) (P1), (P2), (P4)	***erlaubt*** (CW3 (i)) (P1), (P2), (P3)	***verweigert*** (CW3 (ii)) (P1), (P3)
	L(S) = „High“	***verweigert*** (CW1 (ii)) (P4), (P5)	***verweigert*** (CW2 (ii)) (P1), (P4), (P5)		

Tabelle 2: Übersicht der Sicherheitscharakteristika (Security Characteristics)

Lesen von Information Es sei read(S; I; O) der angeforderte Informationsfluss und D der Datenort, an dem das Objekt O aufbewahrt wird.

(CR1) Gibt es keine Informationsflussregel, in der D genannt ist, so wird der Informationsfluss erlaubt. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(CR2) Gibt es eine Informationsflussregel, in der D genannt ist und hat das Sicherheitsattribut C(O) den Wert „Weak“, so wird der Informationsfluss erlaubt. Die Operation Lesen hat in Übereinstimmung mit der in der ausgewählten Informationsflussregel benannten Informationsflussvorschrift zu erfolgen.[2] Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(CR3) Gibt es eine Informationsflussregel, in der D genannt ist und hat das Sicherheitsattribut C(O) den Wert „Strong“, so werden zwei Fälle unterschieden.

(i) Wenn in der ausgewählten Informationsflussregel R das Subjekt S genannt ist, wird der Informationsfluss erlaubt. Die Operation Lesen hat in Übereinstimmung mit der in R benannten Informationsflussvorschrift zu erfolgen.[2] Der Wert des Sicherheitsattributs L(S) wird auf „High“ gesetzt, falls in R das Vertrauenswürdigkeitsflag TF auf „False“ gesetzt ist; andernfalls ändert sich der Wert des Sicherheitsattributs L(S) nicht.

(ii) Wenn in der ausgewählten Informationsflussregel R das Subjekt S nicht genannt ist, wird der Informationsfluss verweigert und der Benutzer wird dahingehend informiert. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

[2] Durch die Verwendung konsistenter Listen von Informationsflussregeln ist gewährleistet, dass die Operation Lesen in der ausgewählten Informationsflussregel genannt ist.

Schreiben von Information Es sei write(S; I; O) der angeforderte Informationsfluss und D der Datenort, an dem das Objekt O aufbewahrt wird.

(CW1) Gibt es keine Informationsflussregel, in der D genannt ist, so werden zwei Fälle unterschieden:

(i) Falls das Sicherheitsattribut L(S) den Wert „Low“ hat, wird der Informationsfluss erlaubt. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(ii) Falls das Sicherheitsattribut L(S) den Wert „High“ hat, wird der Informationsfluss verweigert und der Benutzer wird dahingehend informiert. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(CW2) Gibt es eine Informationsflussregel, in der D genannt ist und hat das Sicherheitsattribut C(O) den Wert „Weak“, so werden zwei Fälle unterschieden:

(i) Falls das Sicherheitsattribut L(S) den Wert „Low“ hat, wird der Informationsfluss erlaubt. Die Operation Schreiben hat in Übereinstimmung mit der in der ausgewählten Informationsflussregel benannten Informationsflussvorschrift zu erfolgen.[3] Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(ii) Falls das Sicherheitsattribut L(S) den Wert „High“ hat, wird der Informationsfluss verweigert und der Benutzer wird dahingehend informiert. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(CW3) Gibt es eine Informationsflussregel, in der D genannt ist und hat das Sicherheitsattribut C(O) den Wert „Strong“, so werden zwei Fälle unterschieden:

(i) Wenn in der ausgewählten Informationsflussregel R das Subjekt S genannt ist, wird der Informationsfluss erlaubt. Die Operation Schreiben hat in Übereinstimmung mit der in R benannten Informationsflussvorschrift zu erfolgen.[3] Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

(ii) Wenn in der ausgewählten Informationsflussregel R das Subjekt nicht genannt S ist, wird der Informationsfluss verweigert und der Benutzer wird dahingehend informiert. Der Wert des Sicherheitsattributs L(S) ändert sich nicht.

Informationsflüsse, die gemäß der Regeln (CW1 (ii)) und (CW2 (ii)) zu verweigern sind, können erlaubt werden, wenn diese Informationsflüsse explizit autorisiert werden (vgl. Prinzip (P5 – Benutzerbestimmbarkeit)). Solche expliziten Autorisierungen werden protokolliert.

[3] Durch die Verwendung konsistenter Listen von Informationsflussregeln ist gewährleistet, dass die Operation Schreiben in der ausgewählten Informationsflussregel genannt ist.

3 EVG-Sicherheitsumgebung

3.1 Beschreibung der Rollen und Werte

3.1.1 Rollen

Der TOE (EVG) kennt folgende Rollen:

EVG-Administrator Ein EVG-Administrator übernimmt die sicherheitsspezifische Konfiguration und Deaktivierung des TOE (EVG). Die Aufgabe des EVG-Administrator umfasst insbesondere die Festlegung der Informationsflussregeln und die Protokollauswertung.

IT-Administrator Ein IT-Administrator installiert den TOE (EVG) und pflegt das übrige IT-System.

IT-Benutzer Ein IT-Benutzer benutzt das IT-System wie gewohnt.

Im Weiteren werden Benutzer, die nicht dazu berechtigt sind, eine der genannten Rollen anzunehmen, unautorisierte Benutzer genannt.

Anwendungsbemerkung 4. Der TOE (EVG) soll die Rollen IT-Benutzer und IT-Administrator voneinander abgrenzen. Hierzu kann vorgesehen werden, dass der TOE (EVG) einen Wartungs- und einen Normalmodus unterscheidet. Jeder Benutzer, der im Normalmodus Zugang zum TOE (EVG) hat, agiert in der Rolle IT-Benutzer, während ein Benutzer, der im Wartungsmodus Zugang zum TOE (EVG) hat, in der Rolle IT-Administrator agiert.

Anwendungsbemerkung 5. Die Rolle EVG-Administrator kann in mehrere Rollen aufgeteilt werden, bspw. um die Festlegung der Informationsflussregeln auf mehrere Verantwortungsbereiche zu verteilen. Der ST-Autor muss dafür sorgen, dass die Konsistenz der eingestellten Informationsflussregeln trotzdem gewahrt bleibt. Mögliche Ansätze hierfür bestehen bspw. in der Vergabe von disjunkten Verantwortungsbereichen oder der Präzisierung hierarchischer Beziehungen zwischen den unterschiedlichen Varianten der Rolle EVG-Administrator.

Anwendungsbemerkung 6. Der ST-Autor kann weitere Rollen einführen, etwa einen EVG-Revisor zur Herstellung der Revisionsfähigkeit des TOE (EVG). Ein EVG-Revisor sollte Protokolldaten durchsehen, auswerten und zurücksetzen können. In diesem Fall sollte ein EVG-Administrator nur die Berechtigung zur Auswertung der Protokolldaten über erlaubte bzw. verweigerte Informationsflüsse erhalten.

3.1.2 Werte

Bei den zu schützenden Werten wird zwischen Primärwerten und Sekundärwerten unterschieden. Primärwerte sind Werte, deren Schutz die eigentliche Aufgabe des TOE (EVG) ist. Sekundärwerte sind zwar schützenswert, existieren allerdings ohne den TOE (EVG) gar nicht. Sind die Sekundärwerte ungeschützt, kann nicht garantiert werden, dass der TOE (EVG) in der Lage ist, die Primärwerte zu schützen.

3.1.2.1 Primärwerte

UserData Zu den UserData gehören die vom IT-Benutzer im Rahmen seiner Tätigkeit verarbeiteten Daten. Sie sind sowohl innerhalb des IT-Systems als auch während der Übertragung zu schützen.

3.1.2.2 Sekundärwerte

TSF-Data Zu den TSF-Data gehören:

ProtocolData Die ProtocolData umfassen alle vom TOE (EVG) protokollierten Ereignisse. Hierzu gehören insbesondere erlaubte und verweigerte Informationsflüsse.

RuleData Die RuleData umfassen die Liste der festgelegten Informationsflussregeln. Eine Informationsflussregel enthält die in Abschnitt 2.5.1 beschriebenen Angaben.

Erläuterung. Durch die Existenz des TOE (EVG) ergeben sich zusätzliche zu schützende Werte. Hierbei handelt es sich u.a. um die RuleData. Weiterhin soll die Funktionsweise des TOE (EVG) überprüfbar sein. Aus diesem Grund sollen stattgefundene und abgewiesene Informationsflüsse protokolliert werden können. Damit erhält ein EVG-Administrator die Möglichkeit zu überprüfen, ob der TOE (EVG) wie beabsichtigt funktioniert.

Im Weiteren werden TSF-Data, die nicht ProtocolData bzw. RuleData sind, andere TSF-Data genannt.

Anwendungsbemerkung 7. Im Falle eines Composite TOE (EVG) können zusätzliche zu schützende Werte vorhanden sein, z.B. Schlüssel, mit denen die kryptographischen Operationen durchgeführt werden. In diesem Falle ergeben sich eventuell zusätzliche Bedrohungen, die sich gegen diese neuen Werte richten. Ein ST-Autor muss dies berücksichtigen.

3.2 Annahmen

A.NoBypass Der TOE (EVG) ist derart in die IT-Umgebung eingebunden, dass alle zu schützenden Informationsflüsse durch den TOE (EVG) geleitet werden.

A.Selection Dem TOE (EVG) werden von der IT-Umgebung verlässliche Zeitstempel und korrekte Informationen zur Identifizierung angeforderter Informationsflüsse, also Subjektidentität (Benutzerkennung und aktive funktionale Einheit), Operation und Datenort, bereitgestellt.

A.Qualification Ein EVG-Administrator und ein IT-Administrator verfügen über eine angemessene Qualifikation.

- Ein EVG-Administrator hat die Befähigung, den TOE (EVG) zu administrieren. Er hat insbesondere die Befähigung, Informationsflussregeln zu definieren und Protokolldaten auszuwerten. Er behandelt die in den Protokollaufzeichnungen enthaltenen Informationen vertraulich.
- Ein IT-Administrator hat die Befähigung, den TOE (EVG) zu installieren.

A.I&A Bevor das IT-System benutzt werden kann, findet eine Identifikation und Authentisierung des Benutzers statt.

Erläuterung. Die Annahme A.I&A trägt maßgeblich dazu bei, dass nur rechtmäßige Benutzer direkt mit dem TOE (EVG) interagieren.

A.NoCapture Laufende Sitzungen eines IT-Benutzers können nicht von einem anderen Benutzer übernommen werden.

Erläuterung. Die Annahme A.NoCapture gewährleistet, dass eine einmal begonnene Sitzung eines IT-Benutzers nicht von anderen Personen (potentiellen Angreifern) fortgeführt werden kann. Damit dies sowohl innerhalb wie außerhalb der regulären Betriebszeiten der IT-Umgebung erreicht werden kann, müssen vorhandene Sicherheitsmechanismen (bspw. Sperren der Sitzung oder Ausschalten des IT-Systems) zweckmäßig eingesetzt werden. Im Rahmen dieses Schutzprofils werden die zur Verfügung zu stellenden Sicherheitsmechanismen nicht genauer spezifiziert (etwa durch Auswahl von seitens der IT-Umgebung bereitzustellenden funktionalen Komponenten aus Teil 2 der CC). Es ist Aufgabe des Herstellers nachzuweisen, auf welche Weise die Annahme A.NoCapture von der IT-Umgebung aufrechterhalten wird. Der Schutz der Sitzungen eines EVG-Administrators wird vom TOE (EVG) gewährleistet (vgl. O.Impersonate). Es sei darauf hingewiesen, dass die Korrektheit der Rollenzuweisung Aufgabe des TOE (EVG) ist und durch die Annahme A.NoCapture nicht sichergestellt werden kann.

A.NoVirus Bösartige Software tritt nicht als Bestandteil von kontrollierten Subjekten in Aktion.

Erläuterung. Die Abwesenheit von bösartiger Software kann praktisch in keiner verfügbaren IT-Umgebung garantiert werden. Ein zu dem vorliegenden Schutzprofil konformer TOE (EVG) leistet einen Beitrag zur Eindämmung der Gefährdung durch bösartige Software, indem diese nur innerhalb der Beschränkungen der Informationsflusskontrolle agieren kann. Die Annahme A.NoVirus ist erforderlich, da die Bewertung der Vertrauenswürdigkeit der Subjekte nicht Bestandteil der Sicherheitsleistung des TOE (EVG) ist.

3.3 Bedrohungen

Nachfolgend werden die grundlegenden Leistungsmerkmale des TOE (EVG) den identifizierten Bedrohungen gegenübergestellt. Damit soll verdeutlicht werden, welche Leistungsmerkmale zur Abwehr welcherart Bedrohungen beitragen sollen. Darüber hinaus wird jede aufgeführte Bedrohung ihrem Urheber zugeordnet. In Tabelle 3 werden die folgende Abkürzungen verwendet: IT-A(dministrator), IT-B(enutzer), EVG-A(dministrator), Un(autorisierter) Be(nutzer), T.Info(rmationFlow), T.Confi(dentiality), T.Mani(pulate), T.Unaw(are), T.Imp(ersonate) , T.Sup(port) und T.Modi(fication).

Leistungsmerkmale	**Urheber der Bedrohungen**			
	IT-A	**IT-B**	**EVG-A**	**UnBe**
Abweisen von Informationsflüssen: Informationsflusskontrolle, Zweckbindung	T.Spy T.Write T.Imp	T.Info T.Spy T.Write T.Imp	—	T.Spy T.Write T.Imp
Sicherung stattfindender Informationsflüsse: Vertraulichkeit, Integrität, Authentizität	T.Confi	T.Info T.Confi	—	T.Read T.Mani T.Confi
Automatische und transparente Anwendung von Sicherheitsfunktionen	—	T.Info T.Unaw	—	T.Read T.Mani
Unterstützung bei der Administration	T.Modi	T.Modi	T.Sup	T.Modi
Protokollierung stattgefundener und abgewiesener Informationsflüsse	T.Spy T.Write	T.Info T.Spy T.Write	—	T.Spy T.Write T.Read T.Mani

Tabelle 3: Zuordnung zwischen Leistungsmerkmalen und Bedrohungen

Anwendungsbemerkung 8. Die Zuordnung von Leistungsmerkmalen zu Bedrohungen ist von informativem Charakter. Sie soll dazu beitragen, die Funktionalität des TOE (EVG) zu veranschaulichen. Für den ST-Autor stehen die nachfolgend definierten Bedrohungen (ebenso wie die Annahmen und organisatorischen Sicherheitspolitiken) im Zentrum der Betrachtung. Diese sind für die Ableitung der Sicherheitsziele und der IT-Sicherheitsanforderungen maßgeblich.

3.3.1 Urheber von Bedrohungen

Aufgrund von Fehlern können ein EVG-Administrator, ein IT-Administrator und ein IT-Benutzer Urheber von Bedrohungen sein. Darüber hinaus können Bedrohungen von einem IT-Administrator, einem IT-Benutzer und von einem unautorisierten Benutzer ggf. unter Verwendung von sogenannter bösartiger Software (z.B. Viren, Trojaner) ausgehen.

3.3.2 Primärbedrohungen

T.InformationFlow Ein IT-Benutzer löst Informationsflüsse aus, die unautorisierten Benutzern die Möglichkeit eröffnen, in Bezug auf Vertraulichkeit, Integrität bzw. Authentizität zu schützende UserData auszuspähen bzw. zu manipulieren.

Erläuterung. Ohne den TOE (EVG) könnte ein IT-Benutzer bspw. versehentlich veranlassen, dass vertrauliche Daten unverschlüsselt über offene Netze transportiert werden.

T.Read In Bezug auf Vertraulichkeit schützenswerte UserData wird während eines stattfindenden Informationsflusses von einem unautorisierten Benutzer gelesen.

Erläuterung. Diese Bedrohung zielt im Besonderen auf die Übertragung von Daten über offene Netze. In erster Linie ist hierbei an die häufig vorkommende Praxis gedacht, Daten, wie z.B. Kreditkartendaten oder Patientendaten unverschlüsselt zu verschicken. Ein unautorisierter Benutzer könnte eine derartige Kommunikation abhören und sich somit sensitive UserData beschaffen.

T.Spy Ein IT-Administrator, ein IT-Benutzer oder ein unautorisierter Benutzer löst (ggf. unter Benutzung bösartiger Software) einen Informationsfluss aus, um in Bezug auf Vertraulichkeit schützenswerte UserData auszuspähen.

Erläuterung. Diese Bedrohung ist analog zur Bedrohung T.Read zu verstehen. Im Unterschied zu dieser geht es aber dabei nicht um das Abhören von ungeschützten Informationskanälen, sondern um das Lesen von gespeicherten UserData (z.B. auf Festplatte oder Diskette).

T.Manipulate In Bezug auf Integrität bzw. Authentizität schützenswerte UserData werden von einem unautorisierten Benutzer während eines stattfindenden Informationsflusses unbemerkt manipuliert.

Erläuterung. Diese Bedrohung zielt in erster Linie auf die Integrität und Authentizität von UserData und nicht auf ihre Vertraulichkeit. UserData sollten, selbst wenn sie an sich nicht vertraulich sind, vor unbemerkter Manipulation geschützt werden können.

T.Write Ein IT-Administrator, ein IT-Benutzer oder ein unautorisierter Benutzer löst (ggf. unter Benutzung bösartiger Software) einen Informationsfluss aus, um in Bezug auf Integrität bzw. Authentizität schützenswerte UserData unbemerkt zu manipulieren.

Erläuterung. Analog zur Bedrohung T.Manipulate.

T.Unaware Aus Unkenntnis bzw. Fahrlässigkeit eines IT-Benutzers werden zur Verfügung stehende Verfahren zum Schutz der Integrität, Authentizität und Vertraulichkeit von UserData gar nicht bzw. nur unzureichend eingesetzt.

Erläuterung. Diese Bedrohung beschreibt die Situation, in der einem IT-Benutzer zwar Mechanismen zur Verfügung stehen, um seine UserData vor unberechtigtem Zugriff zu schützen, er diese aber nicht einsetzt – sei es aus Unkenntnis über die verfügbaren Möglichkeiten oder weil ihm die Anwendung der Schutzmechanismen zu aufwendig oder kompliziert erscheint.

3.3.3 Sekundärbedrohungen

T.Modification Ein IT-Administrator, ein IT-Benutzer oder ein unautorisierter Benutzer (ggf. unter Benutzung bösartiger Software) modifiziert die TSF-Data derart, dass

- festgelegte Sicherheitspolitiken umgangen werden.
- die Integrität und Vertraulichkeit von UserData verloren geht.

Erläuterung. Ein IT-Administrator, ein IT-Benutzer, ein unautorisierter Benutzer (ggf. unter Benutzung bösartiger Software) könnten bspw. die RuleData derart ändern, dass eine von einem EVG-Administrator festgelegte Sicherheitspolitik nicht länger umgesetzt wird.

T.Confidentiality Ein IT-Administrator, ein IT-Benutzer oder ein unautorisierter Benutzer erlangt Kenntnis von den ProtocolData.

Erläuterung. Die unberechtigte Kenntnisnahme von ProtocolData widerspricht grundlegenden Prinzipien des Datenschutzes.

T.Impersonate Eine hierzu nicht berechtigte Person agiert in der Rolle IT-Benutzer bzw. EVG-Administrator.

Erläuterung. Eine Person, die nicht dazu berechtigt ist (ein anderer IT-Benutzer, ein IT-Administrator oder ein unautorisierter Benutzer) kann die Identität eines IT-Benutzers annehmen und an dessen Stelle Informationsflüsse mit kontrollierten Objekten auslösen. Eine Person, die nicht die Berechtigung zur Administration des TOE (EVG) besitzt (ein IT-Benutzer, ein IT-Administrator oder ein unautorisierter Benutzer), erhält die Privilegien der Rolle EVG-Administrator und kann in der Folge den transparent arbeitenden TOE (EVG) abschalten, die RuleData modifizieren oder Kenntnis von den ProtocolData nehmen.

T.Support Aus Unkenntnis bzw. Fahrlässigkeit eines EVG-Administrators wird der TOE (EVG) fehlerhaft administriert.

Erläuterung. Ein EVG-Administrator könnte infolge von Fehlern bei der Administration RuleData derart formulieren, dass die Integrität und Vertraulichkeit der UserData verloren geht.

3.4 Organisatorische Sicherheitspolitiken

P.Appropriation Es muss festgelegt werden können, welche Subjekte (bspw. Applikationen) UserData verarbeiten dürfen.

Erläuterung. Diese organisatorische Sicherheitspolitik ist aus dem folgenden Zweckbindungsprinzip des Datenschutzes abgeleitet:

> Daten dürfen nur zu dem Zweck erhoben, verarbeitet oder genutzt werden, zu dessen Erfüllung sie bestimmt sind. Es muss genau festgelegt werden, wer die Daten wie, mit welchen Hilfsmitteln, in welchen Abständen und zu welchen Zwecken auswerten darf.

4 Sicherheitsziele

Zu Beginn des Kapitels werden die Sicherheitsziele den Leistungsmerkmalen des TOE (EVG) zugeordnet, für deren Realisierung sie von Relevanz sind.

Leistungsmerkmale	Sicherheitsziele
Abweisen von Informationsflüssen: Informationsflusskontrolle, Zweckbindung	O.InformationFlow, O.Impersonate, O.Support, O.EVG-Administration
Sicherung stattfindender Informationsflüsse: Vertraulichkeit, Integrität, Authentizität	O.InformationFlow, O.Disclosure, O.Manipulation, O.Support, O.Impersonate, OE.Disclosure, OE.Manipulation
Automatische und transparente Anwendung von Sicherheitsfunktionen	O.InformationFlow, O.Support, O.EVG-Administration
Unterstützung bei der Administration	O.Support, O.EVG-Administration
Protokollierung stattgefundener und abgewiesener Informationsflüsse	O.Support, O.EVG-Administration

Tabelle 4: Zuordnung zwischen Leistungsmerkmalen und Sicherheitszielen

Anwendungsbemerkung 9. Die Zuordnung von Leistungsmerkmalen zu Sicherheitszielen ist, wie bereits deren Zuordnung zu Bedrohungen, von informativem Charakter. Sie soll dazu beitragen, die Funktionalität des TOE (EVG) zu veranschaulichen. Für den ST-Autor stehen die nachfolgend definierten Sicherheitsziele im Zentrum der Betrachtung. Diese sind für die Ableitung der IT-Sicherheitsanforderungen maßgeblich.

4.1 Sicherheitsziele für den TOE (EVG)

O.InformationFlow Der TOE (EVG) kontrolliert Informationsflüsse gemäß der festgelegten EVG-Sicherheitspolitik. Hierzu gewährleistet der TOE (EVG), dass

- in Bezug auf Vertraulichkeit, Integrität bzw. Authentizität zu schützende Informationen nur unter Einhaltung der EVG-Sicherheitspolitik den kontrollierten Bereich verlassen können.
- dem Zweckbindungsprinzip unterliegende UserData nur von dafür vorgesehenen Subjekten verarbeitet werden können.
- Informationsflüsse mit kontrollierten Datenorten nur von einem EVG-Administrator und von einem IT-Benutzer ausgelöst werden können.

Erläuterung. Der TOE (EVG) muss es gestatten, Informationsflussregeln festzulegen. Die Durchsetzung dieser Informationsflussregeln ist zu erzwingen. Hierzu ist es u.a. erforderlich, dass der TOE (EVG) Subjekte und Objekte identifizieren kann.

Anwendungsbemerkung 10. Die Formulierung von O.InformationFlow legt die Art der kontrollierten Informationsflüsse nicht fest. Die Präzisierung ist Aufgabe des ST-Autors. Damit soll dem Hersteller möglichst viel Flexibilität in Bezug auf Einsatzgebiet und Konstruktion des TOE (EVG) eingeräumt werden.

O.Disclosure Unter Verwendung von Verschlüsselungsverfahren wird durchgesetzt, dass UserData sowohl innerhalb des IT-Systems als auch während der Übertragung vor unberechtigter Kenntnisnahme geschützt werden.

O.Manipulation Unter Verwendung von Signierverfahren wird durchgesetzt, dass die Manipulation von UserData innerhalb des IT-Systems oder während der Übertragung nicht unbemerkt bleibt.

Erläuterung. Die Formulierung der Sicherheitsziele O.Disclosure und O.Manipulation ist identisch zu den entsprechenden Sicherheitszielen für die Umgebung. Dieses ist in Übereinstimmung mit den Common Criteria[4] erforderlich, da beide Sicherheitsziele teilweise dem TOE (EVG) und teilweise dessen Umgebung zuzuordnen sind: Während die Auswahl der Informationsflussvorschriften Aufgabe des TOE (EVG) ist, werden die durch die Informationsflussvorschriften festgelegten kryptographischen Operationen in dessen Umgebung ausgeführt.

O.Support Der TOE (EVG) unterstützt die Tätigkeit eines EVG-Administrators indem

- beim Erzeugen einer neuen Informationsflussregel auf mögliche Konflikte mit bereits vorhandenen Informationsflussregeln hingewiesen wird.
- Ausdrucksmittel (z.B. Wildcards) zur Verfügung gestellt werden, die die Definition von Informationsflussregeln vereinfachen.
- stattgefundene und abgewiesene Informationsflüsse protokollierbar sind und damit Informationen zur Validierung der eingestellten Informationsflussregeln zur Verfügung gestellt werden.

Erläuterung. Die Qualität der Sicherheitsleistung des TOE (EVG) ist maßgeblich von der Zweckmäßigkeit der verwendeten Informationsflussregeln bestimmt. Der Unterstützung bei Generierung und Validierung der RuleData ist daher eine erhebliche Bedeutung beizumessen.

[4] Zitat aus Common Criteria, Teil 1, Abschnitt B.2.5: „Anmerkung: Wenn eine Bedrohung oder organisatorische Sicherheitspolitik teilweise vom TOE (EVG) und teilweise durch dessen Umgebung abgedeckt wird, dann muß das entsprechende Ziel in jeder der beiden Kategorien wiederholt werden.“

O.EVG-Administration Der TOE (EVG) stellt sicher, dass

- nur ein EVG-Administrator die RuleData ändern darf.
- sich der TOE (EVG), einmal installiert und gestartet, nur noch von einem EVG-Administrator deaktivieren lässt.
- nur ein EVG-Administrator von den ProtocolData Kenntnis nehmen kann.

Erläuterung. Die RuleData dürfen nur von Personen festgelegt bzw. geändert werden, die die hierfür erforderliche Kompetenz besitzen. Da der TOE (EVG) transparent arbeitet, ist zu gewährleisten, dass der TOE (EVG) die erwarteten Sicherheitsleistungen auch wirklich erbringt. Die ProtocolData enthalten Details über die Tätigkeit der einzelnen IT-Benutzer, die aus Datenschutzgründen nicht frei zugänglich sein dürfen. Da ein EVG-Administrator die ProtocolData verwenden soll, um die Qualität der festgelegten Informationsflussregeln beurteilen zu können, muss er von den ProtocolData Kenntnis erhalten können.

O.Impersonate Der TOE (EVG) stellt sicher, dass

- nur berechtigte Personen in der Rolle EVG-Administrator agieren können.
- die Rollen IT-Benutzer und IT-Administrator korrekt zugewiesen werden.
- die Rolle IT-Administrator und eine der Rollen IT-Benutzer bzw. EVG-Administrator nicht gleichzeitig agieren können.

Erläuterung. Die Vertrauenswürdigkeit der EVG-Administrationstätigkeit erfordert eine Legitimation durch den TOE (EVG) als Basis für die Rollenzuweisung. Zusätzlich muss der TOE (EVG) sicherstellen, dass die Privilegien der Rolle EVG-Administrator nicht während einer laufenden EVG-Administrationssitzung von hierfür nicht berechtigten Personen übernommen werden können. Ferner ist davon auszugehen, dass ein IT-Administrator (insbesondere im Fall einer Fernadministration des IT-Systems) kein Interesse an der Sicherheitsleistung des TOE (EVG) hat und zudem auf einfache Weise falsche Identitäten vortäuschen kann. Daher soll während der IT-Administrationstätigkeit weder in der Rolle IT-Benutzer noch in der Rolle EVG-Administrator agiert werden können.

4.2 Sicherheitsziele für die Umgebung

OE.Disclosure Unter Verwendung von Verschlüsselungsverfahren wird durchgesetzt, dass UserData sowohl innerhalb des IT-Systems als auch während der Übertragung vor unberechtigter Kenntnisnahme geschützt werden.

OE.Manipulation Unter Verwendung von Signierverfahren wird durchgesetzt, dass eine Manipulation von UserData innerhalb des IT-Systems oder während der Übertragung nicht unbemerkt bleibt.

Anwendungsbemerkung 11. Wenn der kryptographische Betrieb in den TOE (EVG) integriert ist (s. auch Kapitel PP-Anwendungsbemerkungen), so können die Sicherheitsziele OE.Disclosure und OE.Manipulation im ST ersatzlos entfallen, da sie vollständig von den entsprechenden Zielen für den TOE (EVG) erfasst werden.

OE.NoBypass Der TOE (EVG) ist derart in die IT-Umgebung eingebunden, dass alle zu schützenden Informationsflüsse durch den TOE (EVG) geleitet werden.

OE.Selection Dem TOE (EVG) werden von der IT-Umgebung verlässliche Zeitstempel und korrekte Informationen zur Identifizierung angeforderter Informationsflüsse, also Subjektidentität (Benutzerkennung und aktive funktionale Einheit), Operation und Datenort bereitgestellt.
Diese Informationen wie auch die Zeitstempel sind vor Manipulation - auch seitens des IT-Administrators - geschützt.

Erläuterung. Die Verlässlichkeit von Informationen aus einem IT-System hängt grundsätzlich mit der Verlässlichkeit derjenigen Personen zusammen, die das IT-System bzw. Informationen aus dem IT-System administrieren können. Die Manipulationsmöglichkeiten können dabei durchaus auf bestimmte Bereiche oder Aspekte eingeschränkt sein. Im Allgemeinen hat ein IT-Administrator immer die Möglichkeit das IT-System und damit die IT-Umgebung des TOE (EVG) im Rahmen der ihm zugewiesenen Rechte zu manipulieren.
Das obige Ziel an die IT-Umgebung OE.Selection verspricht, dass einem IT-Administrator, der grundsätzlich als potenzieller Angreifer gesehen wird, dies nicht uneingeschränkt möglich ist. Zumindest in Bezug auf Zeitstempel und Informationen zur Identifikation angeforderter Informationsflüsse ist die Verlässlichkeit zu gewährleisten.

OE.Qualification Ein EVG-Administrator und ein IT-Administrator verfügen über eine angemessene Qualifikation.

- Ein EVG-Administrator hat die Befähigung, den TOE (EVG) zu administrieren. Er hat insbesondere die Befähigung, Informationsflussregeln zu definieren und Protokolldaten auszuwerten. Er behandelt die in den Protokollaufzeichnungen enthaltenen Informationen vertraulich.
- Ein IT-Administrator hat die Befähigung, den TOE (EVG) zu installieren.

Erläuterung. Es sei hier auf einige zentrale Aspekte hingewiesen: Ein EVG-Administrator muss wissen, wie die RuleData festzulegen sind, damit die UserData in geeigneter Weise (etwa in Übereinstimmung mit gesetzlichen Regelungen) geschützt werden. Darüber hinaus muss ein EVG-Administrator in der Lage sein, die Protocol-Data auszuwerten.

OE.I&A Bevor das IT-System benutzt werden kann, findet eine Identifikation und Authentisierung statt.

OE.NoCapture Laufende Sitzungen eines IT-Benutzers können nicht von einem anderen Benutzer übernommen werden.

OE.NoVirus Bösartige Software tritt nicht als Bestandteil von kontrollierten Subjekten in Aktion.

Anwendungsbemerkung 12. Möglicherweise kann der TOE (EVG) einen Beitrag zur Durchsetzung des Sicherheitsziels OE.NoVirus leisten, bspw. könnte er bei erkennbarer Aktivität von bösartiger Software geeignete Maßnahmen zur Verhinderung von unerwünschten Informationsflüssen ergreifen (vgl. O.InformationFlow). In einem solchen Fall ist der ST-Autor aufgefordert zu prüfen, ob OE.NoVirus im Abschnitt Sicherheitsziele für den TOE (EVG) wiederholt werden soll.

5 IT-Sicherheitsanforderungen

Dieser Abschnitt beinhaltet funktionale Anforderungen, die von einem zu diesem Schutzprofil konformen Produkt und seiner IT-Umgebung erfüllt sein müssen. Die Anforderungen bestehen aus funktionalen Komponenten des Teils 2 der CC. Tabelle 5 erläutert den Zusammenhang zwischen den CC Funktionsklassen und den Leistungsmerkmalen des TOE (EVG).

Leistungsmerkmale	**Funktionalitätsklassen (nach CC)**
Abweisen von Informationsflüssen: Informationsflusskontrolle, Zweckbindung	FDP (Schutz der Benutzerdaten) FIA (Identifikation und Authentisierung) FTA (EVG-Zugriff)
Sicherung stattfindender Informationsflüsse: Vertraulichkeit, Integrität, Authentizität	FCS (Kryptographische Unterstützung) FDP (Schutz der Benutzerdaten) FIA (Identifikation und Authentisierung) FPT (Schutz der TSF) FTA (EVG-Zugriff)
Transparente und automatische Anwendung von Sicherheitsfunktionen	FMT (Sicherheitsmanagement)
Unterstützung bei der Administration	FAU (Sicherheitsprotokollierung) FMT (Sicherheitsmanagement)
Protokollierung stattgefundener und abgewiesener Informationsflüsse	FAU (Sicherheitsprotokollierung)

Tabelle 5: Zuordnung zwischen Leistungsmerkmalen und CC-Funktionalitätsklassen

5.1 EVG-Sicherheitsanforderungen

Mindest-Stärkestufe der Funktionen

Für die EVG-Sicherheitsfunktionen, die auf einem Wahrscheinlichkeits- oder Permutationsmechanismus beruhen, wird die Mindest-Stärkestufe SOF-Mittel postuliert.

5.1.1 Funktionale Sicherheitsanforderungen an den TOE (EVG)

Tabelle 6 bietet eine Übersicht über die funktionalen Sicherheitsanforderungen, welche vom TOE (EVG) erfüllt werden müssen.

Nr	Komponente	Beschreibung
1.	FAU_GEN.1	Generierung der Protokolldaten
2.	FAU_GEN.2	Verknüpfung der Benutzeridentität
3.	FAU_SAR.1	Durchsicht der Protokollierung
4.	FAU_SAR.2	Eingeschränkte Durchsicht der Protokollierung
5.	FAU_SAR.3	Auswählbare Durchsicht der Protokollierung
6.	FAU_SEL.1	Auswahl der Ereignisse für die Sicherheitsprotokollierung
7.	FAU_STG.1	Geschützte Speicherung des Protokolls
8.	FAU_STG.3	Aktionen im Fall von möglichem Protokolldaten-Verlust
9.	FDP_ETC.1	Export von Benutzerdaten ohne Sicherheitsattribute
10.	FDP_IFC.1	Teilweise Informationsflusskontrolle
11.	FDP_IFF.1	Einfache Sicherheitsattribute
12.	FDP_ITC.1	Import von Benutzerdaten ohne Sicherheitsattribute
13.	FIA_UAU.1	Zeitpunkt der Authentisierung
14.	FIA_UID.1	Zeitpunkt der Identifikation
15.	FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
16.	FMT_MOF.1	Management des Verhaltens der Sicherheitsfunktionen
17.	FMT_MSA.1	Management der Sicherheitsattribute
18.	FMT_MSA.3	Initialisierung statischer Attribute
19a.	FMT_MTD.1A	Management der TSF-Daten
19b.	FMT_MTD.1B	
20.	FMT_MTD.3	Sichere TSF-Daten
21.	FMT_SMF.1	Specification of Management Functions
22.	FMT_SMR.2	Einschränkungen der Sicherheitsrollen
23.	FTA_SSL.3	Durch TSF eingeleitete Beendigung

Tabelle 6: Funktionale Sicherheitsanforderungen an den TOE (EVG)

5.1.1.1 Klasse FAU: Sicherheitsprotokollierung

FAU_GEN.1 Generierung der Protokolldaten

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_GEN.1.1 Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:

a) Starten und Beenden der Protokollierungsfunktionen;

b) Alle protokollierbaren Ereignisse für den Protokollierungsgrad *Minimal*[5] und

c) *Entscheidungen, angeforderte Informationsflüsse zu verweigern (FDP_IFF.1)*[6].

FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; und

b) basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen *die in Tabelle 7 aufgeführte zusätzliche protokollierungsrelevante Information*[7].

Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

Die protokollierbaren Ereignisse für den ausgewählten Protokollierungsgrad sind in Tabelle 7 zusammengefasst.

[5] [Auswahl: Minimal, Einfach, Detailliert, nicht angegeben]
[6] [Zuweisung: sonstige speziell festgelegte protokollierbare Ereignisse]
[7] [Zuweisung: sonstige protokollierungsrelevante Information]

CC-Komponente	Protokollierbares Ereignis	zusätzliche protokollierungsrelevante Information
FAU_SEL.1	Alle Modifizierungen der Protokollierungs-Konfiguration, die während des Betriebs der Protokolldatenerfassungs-Funktionen auftreten.	
FDP_ETC.1	Erfolgreicher Export von Informationen.	
FDP_IFF.1	Entscheidungen, angeforderte Informationsflüsse zu erlauben.	ausgewählte Informationsflussregel, Sicherheitsattribute, explizite Autorisierung
FDP_ITC.1	Erfolgreicher Import von Benutzerdaten, einschließlich der Benutzerattribute.	
FIA_UAU.1	Misslungener Gebrauch des Authentisierungsmechanismus.	
FIA_UID.1	Misslungener Gebrauch des Benutzeridentifikationsmechanismus, einschließlich der bereitgestellten Benutzeridentität.	
FIA_UID.2	Misslungener Gebrauch des Benutzeridentifikationsmechanismus, einschließlich der bereitgestellten Benutzeridentität.	
FMT_MTD.3	Alle zurückgewiesenen Werte von TSF-Daten.	
FMT_SMF.1	Use of the management functions.[8]	
FMT_SMR.2	Modifizierungen der Gruppe von Benutzern, die Teil einer Rolle sind. Misslungene Versuche des Gebrauchs einer Rolle aufgrund bestimmter Bedingungen der Rollen.	
FTA_SSL.3	Beendigung einer interaktiven Sitzung durch den Sitzungssperr-Mechanismus.	

Tabelle 7: Ereignisse für den Protokollierungsgrad „Minimal“

FAU_GEN.2 Verknüpfung der Benutzeridentität

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_GEN.2.1 Die TSF müssen in der Lage sein, jedes protokollierbare Ereignis mit der Identität desjenigen Benutzers zu verknüpfen, der dieses Ereignis verursacht hat.

Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten
FIA_UID.1 Zeitpunkt der Identifikation

[8] Aufgenommen gemäß der *Final Interpretation 065* der CC.

FAU_SAR.1 Durchsicht der Protokollierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_SAR.1.1 Die TSF müssen für *die Rolle EVG-Administrator*[9] die Fähigkeit bereitstellen, *stattgefundene und abgewiesene Informationsflüsse*[10] aus den Protokollaufzeichnungen zu lesen.

FAU_SAR.1.2 Die TSF müssen die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch den Benutzer geeigneten Art und Weise bereitstellen.

Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_SAR.2 Eingeschränkte Durchsicht der Protokollierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_SAR.2.1 Die TSF müssen allen Benutzern Zugriff zum Lesen der Protokollaufzeichnungen verbieten, mit Ausnahme *der Rolle EVG-Administrator*[11].

Abhängigkeiten: FAU_SAR.1 Durchsicht der Protokollierung

FAU_SAR.3 Auswählbare Durchsicht der Protokollierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_SAR.3.1 Die TSF müssen die Fähigkeit der Ausführung von *Suchen und Sortieren*[12] von Protokolldaten auf Grundlage von *Datenorten, Subjekten, Benutzeridentitäten, Zeiträumen, Informationsflussregeln und Sicherheitsattributen*[13] bereitstellen.

Abhängigkeiten: FAU_SAR.1 Durchsicht der Protokollierung

[9] [Zuweisung: autorisierte Benutzer]
[10] [Zuweisung: Liste der Protokollinformationen]
[11] [Verfeinerung: derjenigen Benutzer, denen der Lesezugriff explizit gewährt wurde.]
[12] [Auswahl: Suchen, Sortieren, Ordnen]
[13] [Zuweisung: Kriterien mit logischen Beziehungen]

FAU_SEL.1 Auswahl der Ereignisse für die Sicherheitsprotokollierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_SEL.1.1 Die TSF müssen in der Lage sein, protokollierbare Ereignisse auf Grundlage folgender Attribute in die Menge der protokollierten Ereignisse aufzunehmen bzw. aus dieser auszuschließen:

a) *Objektidentität, Subjektidentität, Benutzeridentität und Ereignisart*[14]

b) *Protokollierungsflag der von der Auswahlfunktion ausgewählten Informationsflussregel*[15].

Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten
FMT_MTD.1 Management der TSF-Daten

FAU_STG.1 Geschützte Speicherung des Protokolls

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_STG.1.1 Die TSF müssen die gespeicherten Protokollaufzeichnungen gegen nichtautorisiertes Löschen schützen.

FAU_STG.1.2 Die TSF müssen Modifizierungen der Protokollaufzeichnungen [Auswahl: *verhindern, erkennen*] können.

Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_STG.3 Aktionen im Fall von möglichem Protokolldaten-Verlust

Ist hierarchisch zu: Keinen anderen Komponenten.

FAU_STG.3.1 Die TSF müssen [Zuweisung: *Aktionen, die im Fall eines möglichen Protokollspeicherfehlers auszuführen sind*], wenn das Protokoll [Zuweisung: *vordefinierte Grenze*] überschreitet.

Abhängigkeiten: FAU_STG.1 Geschützte Speicherung des Protokolls

[14] [Auswahl: Objektidentität, Benutzeridentität, Subjektidentität, Hostrechneridentität, Ereignisart]
[15] [Zuweisung: Liste zusätzlicher Attribute, auf Grundlage derer die Auswahl der Protokollierung erfolgt]

5.1.1.2 Klasse FDP: Schutz der Benutzerdaten

FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute

Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_ETC.1.1 Die TSF müssen die *SFP der benutzerbestimmbaren Informationsflusskontrolle*[16] bei Export von unter Kontrolle der SFPs stehenden Benutzerdaten nach außerhalb des TSC durchsetzen.

FDP_ETC.1.2 Die TSF müssen die Benutzerdaten ohne die mit ihnen verknüpften Sicherheitsattribute exportieren.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle
oder
FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_IFC.1 Teilweise Informationsflusskontrolle

Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_IFC.1.1 Die TSF müssen die SFP der *benutzerbestimmbaren Informationsflusskontrolle*[17] für *alle Subjekte, alle Objekte, aus denen Information zu lesen bzw. in die Information zu schreiben ist, und die Operationen Lesen von Information und Schreiben von Information*[18] durchsetzen.

Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

Erläuterung. Eine Beschreibung der SFP der benutzerbestimmbare Informationsflusskontrolle und der Operationen Lesen von Information und Schreiben von Information findet sich in Abschnitt 2.5.

Anwendungsbemerkung 13. Die Wahl von FDP_IFC.1 stellt eine Minimalanforderung dar, die dem Hersteller möglichst viel Flexibilität einräumen soll (vgl. Anwendungsbemerkung 9). Der ST-Autor kann ggf. FDP_IFC.1 durch die hierarchisch höher stehende Komponente FDP_IFC.2 (Vollständige Informationsflusskontrolle) ersetzen.

[16] [Zuweisung: SFPs für Zugriffskontrolle und/oder SFPs für Informationsflusskontrolle]
[17] [Zuweisung: SFP für Informationsflusskontrolle]
[18] [Zuweisung: Liste der Subjekte, Informationen und der durch die SFP abgedeckten kontrollierten Operationen, die einen Fluss von kontrollierten Informationen zu und von Subjekten bewirken]

FDP_IFF.1 Einfache Sicherheitsattribute

Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_IFF.1.1 Die TSF müssen die SFP der *benutzerbestimmbaren Informationsflusskontrolle*[19] auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen: *Sicherheitslevel des Subjekts und Kontrollstatus des Objekts, aus dem Information zu lesen ist bzw. in das Information zu schreiben ist*[20] durchsetzen.

FDP_IFF.1.2 Die TSF müssen einen über eine kontrollierte Operation erfolgenden Informationsfluss zwischen dem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen[21]: *Die zur Durchsetzung der Sicherheitsprinzipien (security principles) (P1), (P2), (P3) und (P4) geeigneten Sicherheitscharakteristika (security characteristics) sind*

a) Für die Operation Lesen von Information: Wenn die in den Regeln (CR1), (CR2) oder (CR3 (i)) formulierten Voraussetzungen erfüllt sind, ist der Informationsfluss zu erlauben.

b) Für die Operation Schreiben von Information: Wenn die in den Regeln (CW1 (i)), (CW2 (i)), oder (CW3 (i)) formulierten Voraussetzungen erfüllt sind, ist der Informationsfluss zu erlauben.

FDP_IFF.1.3 Die TSF müssen *keine zusätzlichen SFP-Regeln für Informationsflusskontrolle durchsetzen*.[22]

[19] [Zuweisung: SFP für Informationsflusskontrolle]
[20] [Zuweisung: Mindestanzahl und Arten der Sicherheitsattribute]
[21] [Zuweisung: für jede Operation die geforderte auf Sicherheitsattributen basierende Beziehung zwischen Subjekt und Informations-Sicherheitsattributen]
[22] [Zuweisung: zusätzliche SFP-Regeln für Informationsflusskontrolle]

FDP_IFF.1.4 Die TSF müssen *folgende*[23] zusätzlichen SFP-Fähigkeiten bereitstellen.

a) Eine Auswahlfunktion, die nur solche Informationsflussregeln auswählt, die die Eigenschaften (S1) und (S2) haben.

b) In den Informationsflussvorschriften, die Bestandteil der Informationsflussregeln sind, muss mindestens festlegbar sein, dass:

i. Verschlüsselungsverfahren gemäß FCS_COP.1A, FCS_COP.1B und FCS_COP.1C, die die IT-Umgebung bereitstellt, angewendet werden.

ii. Verfahren zum Erstellen und Prüfen elektronischer Signaturen gemäß FCS_COP.1D, FCS_COP.1E und FCS_COP.1F, die die IT-Umgebung bereitstellt, angewendet werden.

c) Für die Operation Lesen von Information: Wenn die in den Regeln (CR2) oder (CR3 (i)) formulierten Voraussetzungen erfüllt sind, hat die Operation Lesen gemäß der in der ausgewählten Informationsflussregel benannten Informationsflussvorschrift zu erfolgen.

d) Für die Operation Schreiben von Information: Wenn die in den Regeln (CW2 (i)) oder (CW3 (i)) formulierten Voraussetzungen erfüllt sind, hat die Operation Schreiben gemäß der in der ausgewählten Informationsflussregel benannten Informationsflussvorschrift zu erfolgen.

e) Die Entscheidung über die Anforderung des Informationsflusses zu protokollieren, falls das Protokollierungsflag PF der ausgewählten Informationsflussregel auf „True“ gesetzt ist bzw. der Informationsfluss gemäß FDP_IFF.1.5 (b) explizit autorisiert wurde.

[23] [Zuweisung: Liste zusätzlicher SFP-Fähigkeiten]

FDP_IFF.1.5 Die TSF müssen einen Informationsfluss auf Grundlage folgender Regeln[24]:

a) Alle Informationsflüsse mit dem Bildschirm und der Tastatur sind zu erlauben.

b) Informationsflüsse sind zu erlauben, wenn die in den Regeln (CW1 (ii)) oder (CW2 (ii)) formulierten Voraussetzungen erfüllt sind und diese von einem hierzu berechtigten Benutzer (mindestens der EVG-Administrator) explizit autorisiert wurden (Sicherheitsprinzip (P5)).

explizit autorisieren.

FDP_IFF.1.6 Die TSF müssen einen Informationsfluss auf Grundlage folgender Regeln[25]:

a) Alle Informationsflüsse mit Objekten, deren Sicherheitsattribut Kontrollstatus den Wert „Strong“ hat, sind zu verweigern, sofern diese nicht von einer der Rollen EVG-Administrator oder IT-Benutzer angefordert werden.

explizit verweigern.

Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle
FMT_MSA.3 Initialisierung statischer Attribute

Erläuterung. Eine Beschreibung der SFP der benutzerbestimmbaren Informationsflusskontrolle einschließlich der zitierten Sicherheitsprinzipien und -charakteristika findet sich in Abschnitt 2.5.

[24] [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit autorisieren]
[25] [Zuweisung: auf Sicherheitsattributen basierende Regeln, die Informationsflüsse explizit verweigern]

FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute

Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_ITC.1.1 Die TSF müssen die *SFP der benutzerbestimmbaren Informationsflusskontrolle*[26] beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen.

FDP_ITC.1.2 Die TSF müssen die mit den Benutzerdaten verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.

FDP_ITC.1.3 Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: *keine*[27].

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder
FDP_IFC.1 Teilweise Informationsflusskontrolle]
FMT_MSA.3 Initialisierung statischer Attribute

Erläuterung. Eine Beschreibung der SFP der benutzerbestimmbaren Informationsflusskontrolle findet sich in Abschnitt 2.5.

[26] [Zuweisung: SFP für Zugriffskontrolle und/oder Informationsflusskontrolle]
[27] [Zuweisung: zusätzliche Importkontrollregeln]

5.1.1.3 Klasse FIA: Identifikation und Authentisierung

In den Komponenten dieser Klasse wird die Erlaubnis zur Ausführung von TSF-vermittelten Aktionen für (rechtmäßige) Benutzer geregelt. Insbesondere sind hiervon die Aktionen zum Durchsetzen der Prinzipien (P1) bis (P5) der SFP der benutzerbestimmbaren Informationsflusskontrolle betroffen. Diese Aktionen entsprechen der regulären Benutzung des TOE (EVG): Der Benutzer fordert Informationsflüsse an und die TSF führen Aktionen zur Kontrolle dieser Informationsflüsse aus, um die Sicherheitsprinzipien (P1) bis (P5) durchzusetzen.
Um die angestrebte Transparenz zu gewährleisten, sollen rechtmäßige Benutzer in der Lage sein, das IT-System wie gewohnt zu verwenden. Die Kontrolle der Informationsflüsse muss daher auf der Grundlage einer Identifikation und Rollenzuweisung (vgl. FMT_SMR.2) stattfinden können, die über Forderungen an die IT-Umgebung hinaus keine eigenständige Authentisierung durch den TOE (EVG) verlangt. Diese Transparenz gilt jedoch nicht für die Freigabe von kryptographischen Schlüsseln; insbesondere, wenn der kryptographische Betrieb in andere Produkte ausgelagert ist.
Die IT-Umgebung muss eine Identifikation und Authentisierung aller Benutzer durchsetzen (vgl. Abschnitt 5.2.2). Auf der Grundlage der von der IT-Umgebung bereitgestellten Benutzerkennungen weist der TOE (EVG) den Benutzern die Rollen IT-Benutzer bzw. IT-Administrator zu (vgl. FMT_SMR.2). Die nachfolgend aufgeführte Komponente FIA_UID.2 stellt sicher, dass die Ausführung von TSF-vermittelten Aktionen erst nach dieser Rollenzuweisung erlaubt ist. Weiterhin gewährleisten die Komponenten FIA_UAU.1 und FIA_UID.1, dass andere als die Aktionen zum Durchsetzen der Prinzipien (P1) bis (P5) der SFP der benutzerbestimmbaren Informationsflusskontrolle nur für den vom TOE (EVG) erfolgreich identifizierten und authentisierten EVG-Administrator erlaubt werden.

FIA_UAU.1 Zeitpunkt der Authentisierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FIA_UAU.1.1 Die TSF müssen die Ausführung der *Aktionen zum Durchsetzen der Prinzipien (P1) bis (P5) der SFP der benutzerbestimmbaren Informationsflusskontrolle*[28] für den Benutzer erlauben, bevor dieser *als EVG-Administrator*[29] authentisiert wird.

FIA_UAU.1.2 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich *als EVG-Administrator*[30] authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

[28] [Zuweisung: Liste der von den TSF vermittelten Aktionen]
[29] [Verfeinerung]
[30] [Verfeinerung]

FIA_UID.1 Zeitpunkt der Identifikation

Ist hierarchisch zu: Keinen anderen Komponenten.

FIA_UID.1.1 Die TSF müssen die Ausführung der *Aktionen zum Durchsetzen der Prinzipien (P1) bis (P5) der SFP der benutzerbestimmbaren Informationsflusskontrolle*[31] für den Benutzer erlauben, bevor dieser *als EVG-Administrator*[32] identifiziert wird.

FIA_UID.1.2 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich *als EVG-Administrator*[33] identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: Keine Abhängigkeiten

FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

Ist hierarchisch zu: FIA_UID.1

FIA_UID.2.1 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich *als IT-Benutzer oder IT-Administrator*[34] identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: Keine Abhängigkeiten

[31] [Zuweisung: Liste der von den TSF vermittelten Aktionen]
[32] [Verfeinerung]
[33] [Verfeinerung]
[34] [Verfeinerung]

5.1.1.4 Klasse FMT: Sicherheitsmanagement

FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MOF.1.1 Die TSF müssen die Fähigkeit zum *Deaktivieren*[35] der Funktionen *zur Durchsetzung der SFP der benutzerbestimmbaren Informationsflusskontrolle*[36] auf *den EVG-Administrator*[37] beschränken.

Abhängigkeiten: FMT_SMR.1 Sicherheitsrollen

FMT_MSA.1 Management der Sicherheitsattribute

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MSA.1.1 Die TSF müssen die *SFP der benutzerbestimmbaren Informationsflusskontrolle*[38] zur Beschränkung der Fähigkeit *zum Ändern der Standardvorgaben*[39] des Sicherheitsattributs *Kontrollstatus eines Objekts*[40] auf *den EVG-Administrator*[41] durchsetzen.

Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle, oder
FDP_IFC.1 Teilweise Informationsflusskontrolle]
FMT_SMF.1 Specification of Management Functions[42]
FMT_SMR.1 Sicherheitsrollen

[35] [Auswahl: Feststellen des Verhaltens von, Deaktivieren, Aktivieren, Modifizieren des Verhaltens]
[36] [Zuweisung: Liste der Funktionen]
[37] [Zuweisung: die autorisierten identifizierten Rollen]
[38] [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle]
[39] [Auswahl: Standardvorgabe ändern, Abfragen, Modifizieren, Löschen, [Zuweisung: andere Optionen]]
[40] [Zuweisung: Liste der Sicherheitsattribute]
[41] [Zuweisung: die autorisierten identifizierten Rollen]
[42] Aufgenommen gemäß der *Final Interpretation 065* der CC.

FMT_MSA.3 Initialisierung statischer Attribute

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MSA.3.1 Die TSF müssen die *SFP für die benutzerbestimmbare Informationsflusskontrolle*[43] zur Bereitstellung von vorgegebenen Standardwerten mit *freizügigen*[44] Eigenschaften für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

FMT_MSA.3.2 Die TSF müssen *keiner Rolle*[45] gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

Abhängigkeiten: FMT_MSA.1 Management der Sicherheitsattribute
FMT_SMR.1 Sicherheitsrollen

Die Komponente wird durch folgende Elemente verfeinert.

FMT_MSA.3.a Bereitstellung freizügiger Standardwerte bedeutet für das Sicherheitsattribut Kontrollstatus, dass der Wert dieses Attributs auf „Weak“ gesetzt wird, falls sich das Objekt an einem Datenort befindet oder erzeugt wird, der nicht zu kontrollieren ist.

FMT_MSA.3.b Bereitstellung freizügiger Standardwerte bedeutet für das Sicherheitsattribut Sicherheitslevel, dass bei Generierung eines neuen Subjekts (bspw. beim Starten einer Applikation) der Wert dieses Attributs auf "Low" gesetzt wird.

[43] [Zuweisung: SFP für Zugriffskontrolle, SFP für Informationsflusskontrolle]
[44] [Auswahl: einschränkenden, freizügigen, anderen Eigenschaften]
[45] [Zuweisung: autorisierten identifizierten Rollen]

FMT_MTD.1A Management der TSF-Daten

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MTD.1A.1 Die TSF müssen die Fähigkeit zum *Modifizieren, Löschen und Ergänzen*[46] von *RuleData und anderen TSF-Data*[47] auf *den EVG-Administrator*[48] beschränken.

Abhängigkeiten: FMT_SMF.1 Specification of Management Functions[49]
FMT_SMR.1 Sicherheitsrollen

FMT_MTD.1B Management der TSF-Daten

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MTD.1B.1 Die TSF müssen die Fähigkeit zum *Abfragen und Zurücksetzen*[50] von *ProtocolData*[51] auf *den EVG-Administrator*[52] beschränken.

Abhängigkeiten: FMT_SMF.1 Specification of Management Functions[53]
FMT_SMR.1 Sicherheitsrollen

[46] [Auswahl: Standardvorgabe ändern, Abfragen, Modifizieren, Löschen, Zurücksetzen, [Zuweisung: andere Operationen]]
[47] [Zuweisung: Liste von TSF-Daten]
[48] [Zuweisung: die autorisierten identifizierten Rollen]
[49] Aufgenommen gemäß der *Final Interpretation 065* der CC.
[50] [Auswahl: Standardvorgabe ändern, Modifizieren, Abfragen, Löschen, Zurücksetzen [Zuweisung: andere Operationen]]
[51] [Zuweisung: Liste von TSF-Daten]
[52] [Zuweisung: die autorisierten identifizierten Rollen]
[53] Aufgenommen gemäß der *Final Interpretation 065* der CC.

FMT_MTD.3 Sichere TSF-Daten

Ist hierarchisch zu: Keinen anderen Komponenten.

FMT_MTD.3.1 Die TSF müssen sicherstellen, dass nur sichere Werte für TSF-Daten akzeptiert werden.

Die Komponente wird durch folgendes Element verfeinert.

FMT_MTD.3.a Die TSF müssen sicherstellen, dass nur konsistente Listen von Informationsflussregeln, d.h. Listen, die den Bedingungen (C1) bis (C4) genügen, akzeptiert werden.

Abhängigkeiten: ADV_SPM.1 Informelles EVG-Sicherheitsmodell
FMT_MTD.1 Management der TSF-Daten

Erläuterung. Der EVG-Administrator kann die TSF-Daten u.a. dadurch modifizieren, dass er Informationsflussregeln formuliert und Listen von Informationsflussregeln einstellt. Die TSF-Daten sind nur dann sicher, wenn ausschließlich konsistente Listen von Informationsflussregeln vom EVG-Administrator eingestellt werden können. Andernfalls kann aufgrund sich widersprechender Informationsflussvorschriften die Verfügbarkeit von Benutzerdaten gefährdet sein bzw. können Informationsflüsse nicht wie gewünscht kontrolliert werden. Die Präzisierung des zugrunde liegenden Konsistenzbegriffs findet sich in Abschnitt 2.5.1.

FMT_SMF.1 Specification of Management Functions[54]

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions[55] :

a) Funktionen, die den EVG-Administrator beim Erstellen von Informationsflussregeln unterstützen.

b) Funktionen, die den EVG-Administrator beim Erstellen von konsistenten Listen von Informationsflussregeln unterstützen.

c) Funktionen, die den EVG-Administrator beim Erstellen von plausiblen Listen von Informationsflussregeln unterstützen.

Die Komponente wird durch folgende Elemente verfeinert.

FMT_SMF.1.a Die TSF sollen folgende Funktionen bereitstellen, die den EVG-Administrator beim Erstellen von Informationsflussregeln unterstützen:

a) Funktionen, die es dem EVG-Administrator ermöglichen, Teile bereits erstellter Informationsflussregeln beim Erstellen neuer Informationsflussregeln zu verwenden (Kopieren und Verschieben).

b) Funktionen, die es dem EVG-Administrator erlauben, Aliase für Informationsflussvorschriften und Listen von Subjekten zu vergeben und diese bei der Erstellung von Informationsflussregeln zu verwenden.

c) Funktionen, die dem EVG-Administrator einerseits Beschreibungsmittel an die Hand geben, um Mengen von Datenorten mit Hilfe von Wildcards kompakt zu beschreiben, und es ihm andererseits ermöglichen, solcherart Beschreibungen bei der Erstellung von Informationsflussregeln zu verwenden.

[54] Diese Komponente wurde in der *Final Interpretation 065* der CC definiert. Eine autorisierte Übersetzung dieser Komponente gibt es nicht. Deshalb ist das englischsprachige Original zitiert worden.
[55] [assignment: list of security management functions to be provided by the TSF]

FMT_SMF.1.b Die TSF sollen folgende Funktionen bereitstellen, die den EVG-Administrator beim Erstellen von konsistenten Listen von Informationsflussregeln, d.h. Listen von Informationsflussregeln, die den Bedingungen (C1) bis (C4) genügen (vgl. Abschnitt 2.5.1), unterstützen:

a) Funktionen, die es dem EVG-Administrator ermöglichen, sich jederzeit einen Überblick über die bisher eingestellten Informationsflussregeln zu verschaffen.

b) Funktionen, die es dem EVG-Administrator gestatten, Listen von Informationsflussregeln nach unterschiedlichen Kriterien zu durchsuchen bzw. zu sortieren.

c) Funktionen, die es dem EVG-Administrator ermöglichen zu erkennen, ob Datenorte gleichzeitig in unterschiedlichen Informationsflussregeln benannt werden und um welche Datenorte und Informationsflussregeln es sich hierbei handelt.

d) Funktionen, die die Eingabemöglichkeiten beim Erstellen von Informationsflussregeln geeignet einschränken.

FMT_SMF.1.c Die TSF sollen folgende Funktionen bereitstellen, die den EVG-Administrator beim Erstellen von plausiblen Listen von Informationsflussregeln unterstützen:

a) Funktionen, die es dem EVG-Administrator gestatten, vorgefertigte Listen von Informationsflussregeln vollständig bzw. teilweise zu übernehmen.

b) Funktionen, die es dem EVG-Administrator ermöglichen, die Stärke (Widerstandsfähigkeit) der in den Informationsflussvorschriften festgelegten Mechanismen zu beurteilen.

c) Funktionen, die es dem EVG-Administrator ermöglichen zu prüfen, ob die Reihenfolge der in den Informationsflussvorschriften festgelegten Einzelschritte zweckmäßig ist.

d) Funktionen, die es dem EVG-Administrator ermöglichen, einen Vorschlag für die zweckmäßige Reihenfolge der in den Informationsflussvorschriften festgelegten Einzelschritte anzufordern bzw. zu übernehmen.

Dependencies: No dependencies.

FMT_SMR.2 Einschränkungen der Sicherheitsrollen

Ist hierarchisch zu: FMT_SMR.1

FMT_SMR.2.1 Die TSF müssen die Rollen *EVG-Administrator, IT-Benutzer und IT-Administrator*[56] erhalten.

FMT_SMR.2.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

FMT_SMR.2.3 Die TSF müssen sicherstellen, dass die Bedingungen *(a) bis (d)*[57] erfüllt werden.

a) Die Zuweisung der Rolle EVG-Administrator erfordert eine explizite Authentisierung.

b) Die Zuweisung der Rolle IT-Benutzer erfolgt durch folgende auslösende Ereignisse:

- *Identifizierung mit einer dem IT-Benutzer zugeordneten Benutzeridentität und damit verbundener Authentisierung durch die IT-Umgebung.*
- *der EVG-Administrator signalisiert das Ende einer Administrationstätigkeit.*

c) Die Zuweisung der Rolle IT-Administrator erfolgt durch folgende auslösende Ereignisse:

- *Identifizierung mit einer dem IT-Administrator zugeordneten Benutzeridentität und damit verbundener Authentisierung durch die IT-Umgebung.*
- *der EVG-Administrator signalisiert den Beginn einer Administrationstätigkeit.*
- *[Zuweisung: Ereignisse, die auf eine Administrationstätigkeit schließen lassen.]*

d) Die Rolle IT-Administrator und eine der Rollen IT-Benutzer bzw. EVG-Administrator können nicht gleichzeitig agieren.

Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

[56] [Zuweisung: die autorisierten identifizierten Rollen]
[57] [Zuweisung: Bedingungen für die verschiedenen Rollen]

Anwendungsbemerkung 14. Bei der Definition zusätzlicher Ereignisse (Zuweisung in FMT_SMR.2.3 (c)), die dem TOE (EVG) von der IT-Umgebung signalisiert werden (wie etwa der Alarm eines Intrusion Detection Systems), soll der ST-Autor prüfen, ob ggf. eine Verfeinerung der Komponente FPT_ITT.1 erforderlich ist, um sicherzustellen, dass diese Signale geschützt an den TOE (EVG) übertragen werden.

5.1.1.5 Klasse FTA: EVG-Zugriff

FTA_SSL.3 Durch TSF eingeleitete Beendigung

Ist hierarchisch zu: Keinen anderen Komponenten.

FTA_SSL.3.1 Die TSF müssen eine interaktive Sitzung *des EVG-Administrators*[58] nach [Zuweisung: *Zeitintervall der Benutzerinaktivität*] beenden.

Abhängigkeiten: Keine Abhängigkeiten

Erläuterung. Die IT-Umgebung stellt typischerweise Sicherheitsmechanismen (bspw. Sperren der Sitzung oder Ausschalten des IT-Systems) zum Schutz von Sitzung eines IT-Benutzers zur Verfügung (siehe OE.NoCapture). Um die Sitzungen eines EVG-Administrators geeignet zu schützen, sind seitens des TOE (EVG) zusätzliche Mechanismen zur Verfügung zu stellen.

[58] [Verfeinerung]

5.1.2 Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

Tabelle 8 bietet eine Übersicht über die Anforderungen an die Vertrauenswürdigkeit, welche vom TOE (EVG) erfüllt werden müssen. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL 2 aus Teil 3 der Common Criteria augmentiert mit der Komponente AVA_MSU.3.

Nr	Komponente	Beschreibung
1.	ACM_CAP.2	Konfigurationsteile
2.	ADO_DEL.1	Auslieferungsprozeduren
3.	ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
4.	ADV_FSP.1	Informelle funktionale Spezifikation
5.	ADV_HLD.1	Beschreibender Entwurf auf hoher Ebene
6.	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
7.	AGD_ADM.1	Systemverwalterhandbuch
8.	AGD_USR.1	Benutzerhandbuch
9.	ATE_COV.1	Nachweis der Testabdeckung
10.	ATE_FUN.1	Funktionales Testen
11.	ATE_IND.2	Unabhängiges Testen – Stichprobenartig
12.	AVA_MSU.3	Analysieren und Testen auf unsichere Zustände
13.	AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
14.	AVA_VLA.1	Schwachstellenanalyse des Entwicklers

Tabelle 8: Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

5.1.2.1 Klasse ACM: Konfigurationsmanagement

ACM_CAP.2 Konfigurationsteile

Abhängigkeiten: Keine Abhängigkeiten

Elemente zu Entwickleraufgaben:

ACM_CAP.2.1D Der Entwickler muss einen Verweisnamen für den TOE (EVG) bereitstellen.

ACM_CAP.2.2D Der Entwickler muss ein CM-System benutzen.

ACM_CAP.2.3D Der Entwickler muss eine CM-Dokumentation bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ACM_CAP.2.1C Der Verweisname für den TOE (EVG) muss für jede Version des TOE (EVG) eindeutig sein.

ACM_CAP.2.2C Der TOE (EVG) muss mit seinem Verweisnamen gekennzeichnet sein.

ACM_CAP.2.3C Die CM-Dokumentation muss ein Konfigurationsverzeichnis enthalten.

ACM_CAP.2.3+C The configuration list shall uniquely identify all configuration items that comprise the TOE.[59]

ACM_CAP.2.4C Das Konfigurationsverzeichnis muss die Konfigurationsteile beschreiben, aus denen der TOE (EVG) besteht.

ACM_CAP.2.5C Die CM-Dokumentation muss die zur eindeutigen Identifikation der Konfigurationsteile verwendete Methode beschreiben.

ACM_CAP.2.6C Das CM-System muss alle Konfigurationsteile eindeutig identifizieren.

[59] Dieses Element wurde gemäß *Final Interpretation 003* der CC ergänzt. Eine autorisierte Übersetzung gibt es nicht. Deshalb ist das englischsprachige Original zitiert worden.

Elemente zu Evaluatoraufgaben:

ACM_CAP.2.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

5.1.2.2 Klasse ADO: Auslieferung und Betrieb

ADO_DEL.1 Auslieferungsprozeduren

Abhängigkeiten: Keine Abhängigkeiten

Elemente zu Entwickleraufgaben:

ADO_DEL.1.1D Der Entwickler muss die Auslieferungsprozeduren des TOE (EVG) oder von Teilen des TOE (EVG) an den Benutzer dokumentieren.

ADO_DEL.1.2D Der Entwickler muss die Auslieferungsprozeduren anwenden.

Elemente zu Inhalt und Form des Nachweises:

ADO_DEL.1.1C Die Auslieferungsdokumentation muss alle Prozeduren beschreiben, die beim Versand von Versionen des TOE (EVG) zum Einsatzort beim Benutzer zur Erhaltung der Sicherheit erforderlich sind.

Elemente zu Evaluatoraufgaben:

ADO_DEL.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren

Abhängigkeiten: AGD_ADM.1 Systemverwalterhandbuch

Elemente zu Entwickleraufgaben:

ADO_IGS.1.1D Entwickler muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Prozeduren dokumentieren.

Elemente zu Inhalt und Form des Nachweises:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.[60]

Elemente zu Evaluatoraufgaben:

ADO_IGS.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADO_IGS.1.2E Der Evaluator muss feststellen, dass die Installations-, Generierungs- und Anlaufprozeduren zu einer sicheren Konfiguration führen.

5.1.2.3 Klasse ADV: Entwicklung

ADV_FSP.1 Informelle funktionale Spezifikation

Abhängigkeiten: ADV_RCR.1 Informeller Nachweis der Übereinstimmung

Elemente zu Entwickleraufgaben:

ADV_FSP.1.1D Der Entwickler muss eine funktionale Spezifikation bereitstellen.

[60] Dieses Element wurde gemäß *Final Interpretation 051* der CC neu formuliert. Eine autorisierte Übersetzung gibt es nicht. Deshalb ist das englischsprachige Original zitiert worden.

Elemente zu Inhalt und Form des Nachweises:

ADV_FSP.1.1C Die funktionale Spezifikation muss die TSF und ihre externen Schnittstellen in einem informellen Stil beschreiben.

ADV_FSP.1.2C Die funktionale Spezifikation muss in sich konsistent sein.

ADV_FSP.1.3C Die funktionale Spezifikation muss den Zweck und die Methode des Gebrauchs aller externen TSF-Schnittstellen beschreiben, einschließlich Details der Wirkungen, Ausnahmen und Fehlermeldungen, wie jeweils angemessen.

ADV_FSP.1.4C Die funktionale Spezifikation muss die TSF vollständig darstellen.

Elemente zu Evaluatoraufgaben:

ADV_FSP.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADV_FSP.1.2E Der Evaluator muss feststellen, dass die funktionale Spezifikation eine getreue und vollständige Umsetzung der funktionalen EVG-Sicherheitsanforderungen ist.

ADV_HLD.1 Beschreibender Entwurf auf hoher Ebene

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation
ADV_RCR.1 Informeller Nachweis der Übereinstimmung

Elemente zu Entwickleraufgaben:

ADV_HLD.1.1D Der Entwickler muss den Entwurf der TSF auf hoher Ebene bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ADV_HLD.1.1C Die Darstellung des Entwurfs auf hoher Ebene muss informell sein.

ADV_HLD.1.2C Der Entwurf auf hoher Ebene muss in sich konsistent sein.

ADV_HLD.1.3C Der Entwurf auf hoher Ebene muss die Strukturen der TSF anhand von Teilsystemen beschreiben.

ADV_HLD.1.4C Der Entwurf auf hoher Ebene muss die von jedem der Teilsysteme der TSF bereitgestellte Sicherheitsfunktionalität beschreiben.

ADV_HLD.1.5C Der Entwurf auf hoher Ebene muss sämtliche den TSF zugrunde liegende Hardware, Firmware und/oder Software angeben und die Funktionen darstellen, die von dem unterstützenden Schutzmechanismus bereitgestellt werden, der in dieser Hardware, Firmware oder Software implementiert ist.

ADV_HLD.1.6C Der Entwurf auf hoher Ebene muss alle Schnittstellen zu den Teilsystemen der TSF identifizieren.

ADV_HLD.1.7C Der Entwurf auf hoher Ebene muss angeben, welche der Schnittstellen zu den Teilsystemen der TSF von außerhalb sichtbar sind.

Elemente zu Evaluatoraufgaben:

ADV_HLD.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADV_HLD.1.2E Der Evaluator muss feststellen, dass der Entwurf auf hoher Ebene eine getreue und vollständige Umsetzung der funktionalen EVG-Sicherheitsanforderungen ist.

ADV_RCR.1 Informeller Nachweis der Übereinstimmung

Abhängigkeiten: Keine Abhängigkeiten

Elemente zu Entwickleraufgaben:

ADV_RCR.1.1D Der Entwickler muss eine Analyse der Übereinstimmung aller benachbarten Paare der bereitgestellten TSF-Darstellungen bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ADV_RCR.1.1C Die Analyse muss für jedes Paar benachbarter TSF-Darstellungen nachweisen, dass die gesamte relevante Sicherheitsfunktionalität der abstrakteren TSF-Darstellung in der weniger abstrakten TSF-Darstellung korrekt und vollständig verfeinert wurde.

Elemente zu Evaluatoraufgaben:

ADV_RCR.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

5.1.2.4 Klasse AGD: Handbücher

AGD_ADM.1 Systemverwalterhandbuch

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation

Elemente zu Entwickleraufgaben:

AGD_ADM.1.1D Der Entwickler muss ein Systemverwalterhandbuch bereitstellen, das an das für Systemverwaltung zuständige Personal gerichtet ist.

Elemente zu Inhalt und Form des Nachweises:

AGD_ADM.1.1C Das Systemverwalterhandbuch muss die Systemverwaltungsfunktionen und Schnittstellen beschreiben, die dem Systemverwalter des TOE (EVG) zur Verfügung stehen.

AGD_ADM.1.2C Das Systemverwalterhandbuch muss beschreiben, wie der TOE (EVG) auf sichere Art und Weise zu verwalten ist.

AGD_ADM.1.3C Das Systemverwalterhandbuch muss Warnungen bezüglich Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_ADM.1.4C Das Systemverwalterhandbuch muss alle Annahmen zum Benutzerverhalten beschreiben, die für den sicheren Betrieb des TOE (EVG) relevant sind.

AGD_ADM.1.5C Das Systemverwalterhandbuch muss alle vom Systemverwalter kontrollierten Sicherheitsparameter beschreiben und dabei, wie jeweils angemessen, sichere Werte angeben.

AGD_ADM.1.6C Das Systemverwalterhandbuch muss jede Art von sicherheitsrelevanten Ereignissen bezüglich der auszuführenden Systemverwaltungsfunktionen beschreiben, einschließlich der Änderungen der Sicherheitseigenschaften von Einheiten, die unter Kontrolle der TSF stehen.

AGD_ADM.1.7C Das Systemverwalterhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_ADM.1.8C Das Systemverwalterhandbuch muss alle Sicherheitsanforderungen an die IT- Umgebung beschreiben, die für den Systemverwalter relevant sind.

Elemente zu Evaluatoraufgaben:

AGD_ADM.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AGD_USR.1 Benutzerhandbuch

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation

Elemente zu Entwickleraufgaben:

AGD_USR.1.1D Der Entwickler muss ein Benutzerhandbuch bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

AGD_USR.1.1C Das Benutzerhandbuch muss die Funktionen und Schnittstellen beschreiben, die den Benutzern des TOE (EVG) zur Verfügung stehen, die nicht für Systemverwaltung zuständig sind.

AGD_USR.1.2C Das Benutzerhandbuch muss den Gebrauch der vom TOE (EVG) bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind, beschreiben.

AGD_USR.1.3C Das Benutzerhandbuch muss Warnungen bezüglich den Benutzern zugänglichen Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_USR.1.4C Das Benutzerhandbuch muss alle Verantwortlichkeiten des Benutzers klar darstellen, die für den sicheren Betrieb des TOE (EVG) notwendig sind, einschließlich derjenigen, die mit den in der Darlegung der EVG-Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen.

AGD_USR.1.5C Das Benutzerhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_USR.1.6C Das Benutzerhandbuch muss alle Sicherheitsanforderungen an die IT- Umgebung beschreiben, die für den Benutzer relevant sind.

Elemente zu Evaluatoraufgaben:

AGD_USR.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

5.1.2.5 Klasse ATE: Testen

ATE_COV.1 Nachweis der Testabdeckung

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation
ATE_FUN.1 Funktionales Testen

Elemente zu Entwickleraufgaben:

ATE_COV.1.1D Der Entwickler muss den Nachweis der Testabdeckung erbringen.

Elemente zu Inhalt und Form des Nachweises:

ATE_COV.1.1C Der Nachweis der Testabdeckung muss die Übereinstimmung zwischen den in der Testdokumentation identifizierten Tests und den TSF, die in der funktionalen Spezifikation beschrieben sind, zeigen.

Elemente zu Evaluatoraufgaben:

ATE_COV.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_FUN.1 Funktionales Testen

Abhängigkeiten: Keine Abhängigkeiten

Elemente zu Entwickleraufgaben:

ATE_FUN.1.1D Der Entwickler muss die TSF testen und die Ergebnisse dokumentieren.

ATE_FUN.1.2D Der Entwickler muss die Testdokumentation bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ATE_FUN.1.1C Die Testdokumentation muss die Testpläne, die Beschreibungen der Testprozeduren, die erwarteten Testergebnisse und die tatsächlichen Testergebnisse enthalten.

ATE_FUN.1.2C Die Testpläne müssen die zu testenden Sicherheitsfunktionen identifizieren und das Ziel der durchzuführenden Tests beschreiben.

ATE_FUN.1.3C Die Beschreibungen der Testprozeduren müssen die durchzuführenden Tests identifizieren und die Testszenarien für jede Sicherheitsfunktion beschreiben. Diese Szenarien müssen alle Ordnungsabhängigkeiten von den Ergebnissen anderer Tests enthalten.

ATE_FUN.1.4C Die erwarteten Testergebnisse müssen die bei einem erfolgreichen Testverlauf zu erwartenden Ergebnisse aufzeigen.

ATE_FUN.1.5C Die Testergebnisse der durch den Entwickler durchgeführten Tests müssen nachweisen, dass sich jede getestete Sicherheitsfunktion (SF) wie spezifiziert verhielt.

Elemente zu Evaluatoraufgaben:

ATE_FUN.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_IND.2 Unabhängiges Testen – Stichprobenartig

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation
AGD_ADM.1 Systemverwalterhandbuch
AGD_USR.1 Benutzerhandbuch
ATE_FUN.1 Funktionales Testen

Elemente zu Entwickleraufgaben:

ATE_IND.2.1D Der Entwickler muss den TOE (EVG) zum Testen bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ATE_IND.2.1C Der TOE (EVG) muss sich zum Testen eignen.

ATE_IND.2.2C Der Entwickler muss eine Menge von Betriebsmitteln bereitstellen, die denen entsprechen, die beim funktionalen Testen der TSF durch den Entwickler verwendet wurden.

Elemente zu Evaluatoraufgaben:

ATE_IND.2.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_IND.2.2E Der Evaluator muss eine Teilmenge der TSF angemessen testen, so dass bestätigt werden kann, dass der TOE (EVG) entsprechend seiner Spezifikation wirkt.

ATE_IND.2.3E Der Evaluator muss zur Verifizierung der Entwicklertestergebnisse eine Stichprobe der in der Testdokumentation enthaltenen Tests durchführen.

5.1.2.6 Klasse AVA: Schwachstellenbewertung

AVA_MSU.3 Analysieren und Testen auf unsichere Zustände

Abhängigkeiten: ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren
ADV_FSP.1 Informelle funktionale Spezifikation
AGD_ADM.1 Systemverwalterhandbuch
AGD_USR.1 Benutzerhandbuch

Elemente zu Entwickleraufgaben:

AVA_MSU.3.1D Der Entwickler muss Handbücher bereitstellen.

AVA_MSU.3.2D Der Entwickler muss eine Analyse der Handbücher dokumentieren.

Elemente zu Inhalt und Form des Nachweises:

AVA_MSU.3.1C Die Handbücher müssen alle möglichen Betriebszustände des TOE (EVG) (einschließlich des Betriebs nach Fehlern oder Fehlbedienung) und deren Folgen für und Auswirkungen auf die Aufrechterhaltung eines sicheren Betriebs identifizieren.

AVA_MSU.3.2C Die Handbücher müssen vollständig, klar, konsistent und vernünftig sein.

AVA_MSU.3.3C Die Handbücher müssen alle Annahmen über die vorgesehene Einsatzumgebung aufführen.

AVA_MSU.3.4C In den Handbüchern müssen alle Anforderungen an die externen Sicherheitsmaßnahmen (einschließlich der externen organisatorischen, materiellen und personellen Kontrollen) aufgeführt sein.

AVA_MSU.3.5C Die Analysedokumentation muss nachweisen, dass die Handbücher vollständig sind.

Elemente zu Evaluatoraufgaben:

AVA_MSU.3.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AVA_MSU.3.2E Der Evaluator muss alle Konfigurations- und Installationsprozeduren und andere ausgewählte Prozeduren wiederholen, um zu bestätigen, dass der TOE (EVG) unter alleiniger Verwendung der mitgelieferten Handbücher sicher konfiguriert und benutzt werden kann.

AVA_MSU.3.3E Der Evaluator muss feststellen, dass der Gebrauch der Handbücher erlaubt, alle unsicheren Zustände zu entdecken.

AVA_MSU.3.4E Der Evaluator muss bestätigen, dass die Analysedokumentation zeigt, dass die Handbücher den sicheren Betrieb in allen Betriebsarten des TOE (EVG) sicherstellt.

AVA_MSU.3.5E Der Evaluator muss unabhängiges Testen durchführen, um festzustellen, dass ein Systemverwalter oder Benutzer, der sich in den Handbüchern auskennt, unter normalen Umständen in der Lage ist festzustellen, ob Konfiguration und Betrieb des TOE (EVG) unsicher sind.

AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation
ADV_HLD.1 Beschreibender Entwurf auf hoher Ebene

Elemente zu Entwickleraufgaben:

AVA_SOF.1.1D Der Entwickler muss eine Analyse der Stärke der EVG-Sicherheitsfunktionen für jeden Mechanismus durchführen, der nach den Angaben in den ST ein Postulat der Stärke der EVG-Sicherheitsfunktionen aufweist.

Elemente zu Inhalt und Form des Nachweises:

AVA_SOF.1.1C Für jeden Mechanismus mit einem Postulat zur Stärke der EVG-Sicherheitsfunktionen muss die Analyse der EVG-Sicherheitsfunktionsstärke nachweisen, dass er die im PP / in den ST definierte Mindeststärkestufe erreicht oder übertrifft.

AVA_SOF.1.2C Für jeden Mechanismus mit einem konkreten Postulat der Stärke der EVG-Sicherheitsfunktion soll die Analyse der Stärke der EVG-Sicherheitsfunktionen nachweisen, dass er die im PP / in den ST definierte spezielle Metrik der Stärke der Funktion erreicht oder übertrifft.

Elemente zu Evaluatoraufgaben:

AVA_SOF.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AVA_SOF.1.2E Der Evaluator muss bestätigen, dass die Stärkepostulate korrekt sind.

AVA_VLA.1 Schwachstellenanalyse des Entwicklers

Abhängigkeiten: ADV_FSP.1 Informelle funktionale Spezifikation
ADV_HLD.1 Beschreibender Entwurf auf hoher Ebene
AGD_ADM.1 Systemverwalterhandbuch
AGD_USR.1 Benutzerhandbuch

Elemente zu Entwickleraufgaben:[61]

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Elemente zu Inhalt und Form des Nachweises:[62]

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Elemente zu Evaluatoraufgaben:

AVA_VLA.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AVA_VLA.1.2E Der Evaluator muss Penetrationstests durchführen, die auf der Schwachstellenanalyse des Entwicklers aufbauen, um sicherzustellen, dass offensichtliche Schwachstellen berücksichtigt wurden.

[61] Die Elemente zu den Entwickleraufgaben sind gemäß *Final Interpretation #051* der CC ersetzt worden. Eine autorisierte deutsche Übersetzung existiert nicht. Daher ist das englischsprachige Original zitiert.
[62] Die Elemente zum Inhalt und zur Form des Nachweises sind gemäß *Final Interpretation #051* der CC ersetzt worden. Eine autorisierte deutsche Übersetzung existiert nicht. Daher ist das englischsprachige Original zitiert.

5.2 Sicherheitsanforderungen an die IT–Umgebung

Tabelle 9 bietet eine Übersicht über die funktionalen Sicherheitsanforderungen, welche von der IT-Umgebung erfüllt werden müssen.

Nr.	Komponente	Beschreibung
1a.	FCS_COP.1A	Kryptographischer Betrieb
1b.	FCS_COP.1B	
1c.	FCS_COP.1C	
1d.	FCS_COP.1D	
1e.	FCS_COP.1E	
1f.	FCS_COP.1F	
2.	FIA_UAU.2A	Benutzerauthentisierung vor jeglicher Aktion
3.	FIA_UID.2A	Benutzeridentifikation vor jeglicher Aktion
4.	FPT_RVM.1	Nichtumgehbarkeit der TSP
5.	FPT_ITT.1	Einfacher Schutz bei internem TSF-Datenaustausch
6.	FPT_SEP.1	TSF-Bereichsseparierung
7.	FPT_STM.1	Verlässlicher Zeitstempel

Tabelle 9: Funktionale Sicherheitsanforderungen an die IT-Umgebung.

Anwendungsbemerkung 15. Durch das vorliegende Schutzprofil soll der Hersteller in der Gestaltung des kryptographischen Schlüsselmanagements nicht eingeschränkt werden. Daher sind die von den Iterationen der Komponente FCS_COP.1 ausgehenden Abhängigkeiten nicht aufgelöst. Es ist die Aufgabe des ST-Autors, geeignete Anforderungen an das kryptographische Schlüsselmanagement zu ergänzen.

5.2.1 Klasse FCS: Kryptographische Unterstützung

Die der nachfolgenden Iteration der Komponente FCS_COP.1 zugrunde liegende Auswahl von kryptographischen Algorithmen folgt den vom BSI im Rahmen der SPHINX-Spezifikation verpflichtend geforderten Vorgaben [SPHINX, Kap. 11]. Darüber hinaus wird die Unterstützung des kryptographischen Algorithmus „Advanced Encryption Standard (AES)“ gefordert. Neben der Berücksichtigung der geforderten Mindestschlüssellängen ist die Wahl aller Parameter (Padding, Wahl der Primfaktoren, Zufallszahlengenerator, etc.) so zu gestalten, dass die im Rahmen dieses Schutzprofils geforderte Mindeststärkestufe SOF-Mittel erreicht wird.

Anwendungsbemerkung 16. Zusätzlich zu den angegebenen können weitere kryptographische Algorithmen unterstützt werden. Dabei sollen die Empfehlungen des BSI, insbesondere die regelmäßig im Bundesanzeiger veröffentlichten „Geeigneten Kryptoalgorithmen“, berücksichtigt werden. Beispielsweise kann das im Rahmen der SPHINX-Spezifikation empfohlene Schema RSAES-OAEP [SPHINX, Abschnitt 11.4.1.2] ergänzt werden.

Anwendungsbemerkung 17. Alle vom TOE (EVG) verwendeten kryptographischen Algorithmen müssen grundsätzlich die Mindeststärkestufe SOF-Mittel erreichen. Um dieser Forderung gerecht zu werden, kann es notwendig sein, einzelne der in diesem Schutzprofil geforderten kryptographischen Algorithmen durch andere zu ersetzen bzw. deren Parameter geeignet anzupassen. Dieser Fall tritt ein, wenn – bedingt durch den technischen Fortschritt – einer der hier geforderten kryptographischen Algorithmen nicht mehr die Stärkestufe SOF-Mittel erreicht. Bei der Auswahl von Alternativen sollen die jeweils aktuellen Empfehlungen des BSI berücksichtigt werden. Übergangsweise kann es erforderlich sein, kryptographische Algorithmen, die nicht mehr die Stärkestufe SOF-Mittel erreichen, weiterhin zu unterstützen. In einem solchen Fall muß deren Verwendung durch den TOE (EVG) standardmäßig abgeschaltet sein. Begleitet vom einem deutlichen Hinweis auf die Schäche des Algorithmus soll zur Freischaltung ein expliziter Eingriff des EVG-Administrators erforderlich sein.

FCS_COP.1A Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1A.1 Die *IT-Umgebung muss*[63] *Verschlüsseln und Entschlüsseln von UserData*[64] gemäß eines spezifizierten kryptographischen Algorithmus: *AES*[65] und kryptographischer Schlüssellängen *von mindestens 128 Bit*[66], die den folgenden *Normen: [FIPS 197]*[67] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

FCS_COP.1B Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1B.1 Die *IT-Umgebung muss*[68] *Verschlüsseln und Entschlüsseln von UserData*[69] gemäß eines spezifizierten kryptographischen Algorithmus: *Triple-DES im CBC-Modus*[70] und kryptographischer Schlüssellängen *von 128 Bit (112 Bit effektiv)*[71], die den folgenden *Normen: [FIPS 46-3], [FIPS 81], [ISO/IEC 10116] [X9.52],*[72] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

[63] [Verfeinerung: TSF müssen]
[64] [Zuweisung: Liste der kryptographischen Operationen]
[65] [Zuweisung: kryptographischer Algorithmus]
[66] [Zuweisung: kryptographische Schlüssellänge]
[67] [Zuweisung: Liste der Normen]
[68] [Verfeinerung: TSF müssen]
[69] [Zuweisung: Liste der kryptographischen Operationen]
[70] [Zuweisung: kryptographischer Algorithmus]
[71] [Zuweisung: kryptographische Schlüssellänge]
[72] [Zuweisung: Liste der Normen]

FCS_COP.1C Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1C.1 Die *IT-Umgebung muss*[73] *Verschlüsseln und Entschlüsseln von Nachrichtenschlüsseln*[74] gemäß eines spezifizierten kryptographischen Algorithmus: *RSA*[75] und kryptographischer Schlüssellängen *von mindestens 1024 Bit*[76], die den folgenden *Normen: [PKCS #1]*[77] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

FCS_COP.1D Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1D.1 Die *IT-Umgebung muss*[78] *das Berechnen von Hashwerten für UserData*[79] gemäß eines spezifizierten kryptographischen Algorithmus: *SHA-1*[80] und kryptographischer Schlüssellängen: *Keine*[81], die den folgenden *Normen: [FIPS 180-1]*[82] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

[73] [Verfeinerung: TSF müssen]
[74] [Zuweisung: Liste der kryptographischen Operationen]
[75] [Zuweisung: kryptographischer Algorithmus]
[76] [Zuweisung: kryptographische Schlüssellänge]
[77] [Zuweisung: Liste der Normen]
[78] [Verfeinerung: TSF müssen]
[79] [Zuweisung: Liste der kryptographischen Operationen]
[80] [Zuweisung: kryptographischer Algorithmus]
[81] [Zuweisung: kryptographische Schlüssellänge]
[82] [Zuweisung: Liste der Normen]

FCS_COP.1E Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1E.1 Die *IT-Umgebung muss*[83] *das Erzeugen und das Prüfen von Signaturen für UserData*[84] gemäß eines spezifizierten kryptographischen Algorithmus: *RSA*[85] und kryptographischer Schlüssellängen *von mindestens 1024 Bit*[86], die den folgenden *Normen: [PKCS #1]*[87] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

FCS_COP.1F Kryptographischer Betrieb

Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1F.1 Die *IT-Umgebung muss*[88] *das Erzeugen und das Prüfen von Signaturen für UserData*[89] gemäß eines spezifizierten kryptographischen Algorithmus: *SHA-1 mit RSA*[90] und kryptographischer Schlüssellängen *von mindestens 1024 Bit*[91], die den folgenden *Normen: [PKCS #1], [FIPS 180-1]*[92] entsprechen, durchführen.

Abhängigkeiten: [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

[83] [Verfeinerung: TSF müssen]
[84] [Zuweisung: Liste der kryptographischen Operationen]
[85] [Zuweisung: kryptographischer Algorithmus]
[86] [Zuweisung: kryptographische Schlüssellänge]
[87] [Zuweisung: Liste der Normen]
[88] [Verfeinerung: TSF müssen]
[89] [Zuweisung: Liste der kryptographischen Operationen]
[90] [Zuweisung: kryptographischer Algorithmus]
[91] [Zuweisung: kryptographische Schlüssellänge]
[92] [Zuweisung: Liste der Normen]

5.2.2 Klasse FIA: Identifikation und Authentisierung

Das Zusammenwirken der nachfolgend aufgeführten Komponenten mit den funktionalen Anforderungen an den TOE (EVG) ist in Kap. 5.1.1.3 erläutert. Die Identifikation und Authentisierung der rechtmäßigen Benutzer erfolgt durch die IT-Umgebung. Jede Form der Rollenzuweisung wird durch den TOE (EVG) vorgenommen.

FIA_UAU.2A Benutzerauthentisierung vor jeglicher Aktion

Ist hierarchisch zu: FIA_UAU.1

FIA_UAU.2A.1 Die *IT-Umgebung muss*[93] erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: FIA_UID.1

FIA_UID.2A Benutzeridentifikation vor jeglicher Aktion

Ist hierarchisch zu: FIA_UID.1

FIA_UID.2A.1 Die *IT-Umgebung muss*[94] erfordern, dass jeder Benutzer erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: Keine Abhängigkeiten

Erläuterung: Diese Anforderungen stellen sicher, dass sowohl eine erfolgreiche Authentisierung als auch eine erfolgreiche Identifizierung von der IT-Umgebung gewährleistet wird, bevor TSF-vermittelte Aktionen erlaubt werden. Es muss sichergestellt werden, dass ein IT-Administrator trotz seiner prinzipiellen Möglichkeiten das IT-System zu manipulieren, die Identifizierung und die Authentifizierung bei der in diesem PP geforderten Mindeststärkestufe der Funktionen und bei dem in der Schwachstellenbewertung angenommenen Angriffspotential nicht überwinden kann. Das Schutzprofil überlässt die Hinzunahme weiterer funktionaler Sicherheitsanforderungen (zum Management der FIA) zur Gewährleistung obiger Bedingungen dem ST-Autor, da diese von der Art des TOE (EVG) und der Einsatzumgebungen abhängen und somit auf der Abstraktionsebene des Schutzprofils noch nicht spezifiziert werden können.

[93] [Verfeinerung: TSF müssen]
[94] [Verfeinerung: TSF müssen]

5.2.3 Klasse FPT: Schutz der TSF

FPT_ITT.1 Einfacher Schutz bei internem TSF-Datenaustausch

Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_ITT.1.1 Die *IT-Umgebung muss*[95] *Zeitstempel und die zur Identifikation von angeforderten Informationsflüssen wesentlichen Informationen (Subjektidentität, also Benutzerkennung und aktive funktionale Einheit, Operation und Datenort)*[96] während der Übertragung *zum TOE (EVG)*[97] gegen *Modifizierung*[98] schützen.

Abhängigkeiten: Keine Abhängigkeiten

FPT_RVM.1 Nichtumgehbarkeit der TSP

Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_RVM.1.1 Die *IT-Umgebung muss*[99] sicherstellen, dass TSP-Funktionen zur Durchsetzung aktiv und erfolgreich sind, bevor den Funktionen innerhalb des TSC die Ausführung gestattet wird.

Abhängigkeiten: Keine Abhängigkeiten

Erläuterung. Diese Anforderung stellt sicher, dass die IT-Umgebung den TOE (EVG) aktiviert, bevor Benutzer Informationsflüsse anfordern können.

[95] [Verfeinerung: TSF müssen]
[96] [Verfeinerung: TSF-Daten]
[97] [Verfeinerung: zwischen getrennten EVG-Teilen]
[98] [Auswahl: Preisgabe, Modifizierung]
[99] [Verfeinerung: TSF müssen]

FPT_SEP.1 TSF-Bereichsseparierung

Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_SEP.1.1 Die *IT-Umgebung muss*[100] einen Sicherheitsbereich *für die TOE (EVG)*[101] Ausführung aufrechterhalten, der *die TSF*[102] vor Eingriffen und Manipulationen durch nichtvertrauenswürdige Subjekte schützt.

FPT_SEP.1.2 Die *IT-Umgebung muss*[103] die Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen.

Abhängigkeiten: Keine Abhängigkeiten

Erläuterung. FPT_SEP.1 dient dem Zweck zu verhindern, dass potentielle Angreifer den internen Zustand des TOE (EVG) derart modifizieren können, dass die TSF umgangen, deaktiviert, verfälscht oder außer Kraft gesetzt werden.

FPT_STM.1 Verlässlicher Zeitstempel

Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_STM.1.1 Die *IT-Umgebung soll*[104] einen verlässlichen Zeitstempel für *den Gebrauch durch die TSF*[105] bereitstellen.

Abhängigkeiten: Keine Abhängigkeiten

Erläuterung. Die Anforderungen FPT_STM.1 und FPT_ITT.1 stellen sicher, dass einerseits verlässliche Zeitstempel bereitgestellt werden und andererseits Zeitstempel sowie zur Identifikation von angeforderten Informationsflüssen wesentliche Informationen während der Übertragung zum TOE (EVG) gegen Modifizierung geschützt sind.Es muss sichergestellt werden, dass ein IT-Administrator trotz seiner prinzipiellen Möglichkeiten das IT-System zu manipulieren, weder die Bereitstellung eines verlässlichen Zeitstempels noch den Schutz von Informationen gegen Modifizierung während der Übertragung zum TOE (EVG) bei der in diesem PP geforderten Mindeststärkestufe der Funktionen und bei dem in der Schwachstellenbewertung angenommenen Angriffspotential überwinden kann. Die Hinzunahme weiterer funktionaler Sicherheitsanforderungen (zum Management der FPT) zur Gewährleistung obiger Bedingungen wird dem ST-Autor überlassen, da diese von der Art des TOE (EVG) und der Einsatzumgebungen abhängen und somit auf der Abstraktionsebene des PP noch nicht spezifiziert werden können.

[100] [Verfeinerung: TSF müssen]
[101] [Verfeinerung: ihre eigene]
[102] [Verfeinerung: diese]
[103] [Verfeinerung: TSF müssen]
[104] [Verfeinerung: TSF sollen]
[105] [Verfeinerung: den Eigengebrauch]

6 PP–Anwendungsbemerkungen

Die einzelnen Abschnitte des Schutzprofils enthalten entsprechend gekennzeichnete Anwendungsbemerkungen. Darüber hinaus wird auf das Folgende hingewiesen.

Der TOE (EVG) verwendet kryptographische Funktionen, ob als Hardware, Firmware und/oder Software implementiert, um seine Sicherheitsziele abzudecken. Es wird nicht verlangt, dass der TOE (EVG) selbst kryptographische Unterstützung bietet. Das Schutzprofil ist so konzipiert, dass diese Funktionalität durch ein anderes vertrauenswürdiges IT-Produkt (z.B. Smartcards) erbracht werden kann.

Der Hersteller hat dafür Sorge zu tragen, dass die zu verschlüsselnden, bzw. zu signierenden Daten während der Übertragung zu den Komponenten für den kryptographischen Betrieb geeignet geschützt werden. Zu diesem Zweck kann der ST-Autor ggf. die folgenden funktionalen Anforderungskomponenten in das ST aufnehmen:

- FDP_UCT.1 (Einfache Vertraulichkeit des Datenaustausches)
- FDP_UIT.1 (Schutz der Benutzerdatenintegrität bei Inter-TSF Transfer)
- FTP_ITC.1 (Inter-TSF Vertrauenswürdiger Kanal)

Sind die Funktionen für den kryptographischen Betrieb vollständig bzw. teilweise Bestandteil des Produkts (Composite TOE (EVG)), so werden die genannten Anforderungskomponenten nicht bzw. nur zum Teil benötigt. Wegen der vielfältigen Realisierungsmöglichkeiten wird ihre Verwendung in diesem Schutzprofil nicht vorgeschrieben.

Wenn die Funktionen für den kryptographischen Betrieb vollständig innerhalb des TOE (EVG) realisiert werden, so ist die Komponente FCS_COP.1 (sowie alle direkt oder indirekt abhängigen Anforderungskomponenten) im ST in den Abschnitt funktionale Sicherheitsanforderungen an den TOE (EVG) zu verschieben. Weiterhin sind die Sicherheitsziele OE.Disclosure und OE.Manipulation ersatzlos zu streichen, da sie vollständig von den Zielen O.Disclosure und O.Manipulation erfasst werden.

7 Erklärung

7.1 Erklärung der Sicherheitsziele

Tabelle 10 zeigt, dass jedes in Kap. 4 identifizierte Sicherheitsziel mindestens einer Bedrohung entgegenwirkt bzw. mindestens eine Annahme oder organisatorische Sicherheitspolitik abdeckt.

Aspekte der EVG-Sicherheitsumgebung	Sicherheitsziele
A.NoBypass	OE.NoBypass
A.Selection	OE.Selection
A.Qualification	OE.Qualification
A.I&A	OE.I&A
A.NoCapture	OE.NoCapture
A.NoVirus	OE.NoVirus
T.InformationFlow	O.InformationFlow, O.Support, O.EVG-Administration, OE.Qualification, OE.Selection, OE.NoBypass
T.Read	O.InformationFlow, O.Disclosure, OE.Disclosure
T.Spy	O.InformationFlow, O.Disclosure, OE.Disclosure, O.Impersonate, OE.I&A, OE.NoCapture, OE.NoBypass, OE.NoVirus, OE.Selection
T.Manipulate	O.InformationFlow, O.Manipulation, OE.Manipulation
T.Write	O.InformationFlow, O.Manipulation, OE.Manipulation, O.Impersonate, OE.I&A, OE.NoCapture, OE.NoBypass, OE.NoVirus, OE.Selection
T.Unaware	O.InformationFlow, O.Disclosure, OE.Disclosure, O.Manipulation, OE.Manipulation, O.Support, O.EVG-Administration, OE.Qualification
T.Modification	O.EVG-Administration, O.Impersonate, OE.I&A
T.Confidentiality	O.EVG-Administration, O.Impersonate, OE.I&A, OE.Qualification
T.Impersonate	O.Impersonate, OE.I&A, OE.NoCapture, OE.Selection
T.Support	O.Support, OE.Qualification
P.Appropriation	O.InformationFlow, O.Support, O.EVG-Administration, OE.Qualification, OE.NoBypass, OE.Selection

Tabelle 10: Abdeckung der EVG-Sicherheitsumgebung durch die Sicherheitsziele

Nachfolgend wird für jeden Aspekt der in Kap. 3 dargelegten Sicherheitsumgebung erklärt, warum er von den in Tabelle 10 aufgeführten Sicherheitszielen abgedeckt wird.

A.NoBypass

Durch die Formulierung ist offenbar, dass die Annahme A.NoBypass direkt von dem Sicherheitsziel OE.NoBypass abgedeckt wird.

A.Selection

Durch die Formulierung ist offenbar, dass die Annahme A.Selection direkt von dem Sicherheitsziel OE.Selection abgedeckt wird.

A.Qualification

Durch die Formulierung ist offenbar, dass die Annahme A.Qualification direkt von dem Sicherheitsziel OE.Qualification abgedeckt wird.

A.I&A

Durch die Formulierung ist offenbar, dass die Annahme A.I&A direkt von dem Sicherheitsziel OE.I&A abgedeckt wird.

A.NoCapture

Durch die Formulierung ist offenbar, dass die Annahme A.NoCapture direkt von dem Sicherheitsziel OE.NoCapture abgedeckt wird.

Erläuterung. Es sei an dieser Stelle darauf hingewiesen, dass die Annahme A.NoCapture zwar verhindert, dass eine einmal begonnene Sitzung eines Benutzers von einer unberechtigten Person fortgeführt werden kann, aber keinen Schutz gegen den Aufbau einer neuen Sitzung im Namen dieses Benutzers bietet. Durch die Annahme A.I&A ist allerdings gewährleistet, dass dazu eine eigene Identifikation und Authentisierung des Benutzers notwendig wäre. Damit verhindert das Zusammenwirken von A.I&A und A.NoCapture, dass im Namen des Benutzers Informationsflüsse von dazu nicht berechtigten Personen ausgelöst werden.

A.NoVirus

Durch die Formulierung ist offenbar, dass die Annahme A.NoVirus direkt von dem Sicherheitsziel OE.NoVirus abgedeckt wird.

T.InformationFlow

Das Sicherheitsziel O.InformationFlow stellt sicher, dass Informationsflüsse nur im Einklang mit der festgelegten Sicherheitspolitik erfolgen können. Die Ziele O.Support, O.EVG-Administration und OE.Qualification sorgen dafür, dass die festgelegte Sicherheitspolitik dem Schutzbedürfnis des IT-Benutzers entspricht. Schließlich ist durch OE.Selection und OE.NoBypass gewährleistet, dass kein Informationsfluss vom TOE (EVG) unbemerkt stattfinden kann.

T.Read

Die Sicherheitsziele O.Disclosure bzw. OE.Disclosure verhindern durch Verschlüsselung im Zusammenspiel mit O.InformationFlow die Verletzung der Vertraulichkeit von UserData.

T.Spy

Die Sicherheitsziele OE.I&A, OE.NoCapture, O.InformationFlow und O.Impersonate gewährleisten, dass unautorisierte Benutzer bzw. der IT-Administrator auf direktem Wege keine Informationsflüsse mit kontrollierten Objekten auslösen können und dass der IT-Benutzer ausschließlich Informationsflüsse auslösen kann, die seiner Benutzeridentität zugeordnet sind. Im Zusammenhang mit OE.NoBypass und OE.Selection sorgen die Ziele O.InformationFlow und O.Disclosure bzw. OE.Disclosure dafür, dass bösartige Software nur dann Informationsflüsse auslösen kann, durch die die Vertraulichkeit der UserData verletzt wird, wenn sie als Bestandteil eines kontrollierten Subjekts in Aktion tritt. Dies wird durch OE.NoVirus verhindert.

T.Manipulate

Die Sicherheitsziele O.Manipulation bzw. OE.Manipulation verhindern mit elektronischen Signaturen im Zusammenspiel mit O.InformationFlow die unbemerkte Verletzung der Integrität oder Authentizität von UserData bei einem stattfindenden Informationsfluss.

T.Write

Die Sicherheitsziele OE.I&A, OE.NoCapture, O.InformationFlow und O.Impersonate gewährleisten, dass unautorisierte Benutzer bzw. der IT-Administrator auf direktem Wege keine Informationsflüsse mit kontrollierten Objekten auslösen können und dass der IT-Benutzer ausschließlich Informationsflüsse auslösen kann, die seiner Benutzeridentität zugeordnet sind. Im Zusammenhang mit OE.NoBypass und OE.Selection sorgen die Ziele O.InformationFlow und O.Manipulation bzw. OE.Manipulation dafür, dass bösartige Software nur dann Informationsflüsse auslösen kann, durch die die Integrität der UserData unbemerkt verletzt wird, wenn sie als Bestandteil eines kontrollierten Subjekts in Aktion tritt. Dies wird durch OE.NoVirus verhindert.

T.Unaware

Die Sicherheitsziele O.Disclosure bzw. OE.Disclosure und O.Manipulation bzw. OE.Manipulation im Zusammenhang mit O.InformationFlow gewährleisten die Umsetzung der festgelegten Sicherheitspolitik zum Schutz der Integrität, Authentizität und Vertraulichkeit der UserData ohne den IT-Benutzer mit der Durchführung der notwendigen Maßnahmen zu belasten. Die Ziele O.Support, O.EVG-Administration und OE.Qualification sorgen dafür, dass die festgelegte Sicherheitspolitik dem Schutzbedürfnis des IT-Benutzers entspricht.

T.Modification

Der Bedrohung T.Modification ist durch die Sicherung der Integrität der TSF-Data entgegenzuwirken. Dies wird durch die Sicherheitsziele O.EVG-Administration, O.Impersonate und OE.I&A gewährleistet.

T.Confidentiality

Die Sicherheitsziele O.EVG-Administration, O.Impersonate und OE.I&A gewährleisten, dass der TOE (EVG) die Kenntnisnahme der ProtocolData auf die Rolle des EVG-Administrator beschränkt. Im Zusammenspiel mit dem Sicherheitsziel OE.Qualification stellt dies sicher, dass andere Personen keine Kenntnis von den ProtocolData erlangen können.

T.Impersonate

Die korrekte Identifizierung und Authentisierung des EVG-Administrator als Grundlage für die Rollenzuweisung im TOE (EVG) sowie die Erhaltung der Korrektheit dieser Rollenzuweisung wird durch O.Impersonate gewährleistet. Die Sicherheitsziele OE.I&A und O.Impersonate sichern die korrekte Zuweisung der Rolle IT-Benutzer und im Zusammenwirken mit OE.NoCapture die Erhaltung der Korrektheit dieser Rollenzuweisung. Schließlich garantiert OE.Selection, dass selbst ein als potenzieller Angreifer anzusehender IT-Administrator derartige Informationen nicht manipulieren kann.

T.Support

Der Bedrohung T.Support ist durch Unterstützung des EVG-Administrator bei der Administration des TOE (EVG) entgegenzuwirken. Dies wird durch die Sicherheitsziele O.Support und OE.Qualification gewährleistet.

P.Appropriation

Das Sicherheitsziel O.InformationFlow stellt sicher, dass UserData nur von den dafür in der Sicherheitspolitik festgelegten Subjekten verarbeitet werden können. Die Ziele O.Support, O.EVG-Administration und OE.Qualification sorgen dafür, dass die festgelegte Sicherheitspolitik dem Schutzbedürfnis des IT-Benutzers entspricht. Schließlich ist durch OE.Selection und OE.NoBypass gewährleistet, dass kein Informationsfluss vom TOE (EVG) unbemerkt stattfinden kann.

7.2 Erklärung der Sicherheitsanforderungen

7.2.1 Erklärung der funktionalen Sicherheitsanforderungen

Tabelle 11 zeigt, dass jede in Kap. 5 identifizierte funktionale Sicherheitsanforderung der Erfüllung mindestens eines (IT-)Sicherheitsziels dient.

(IT-)Sicherheitsziele	Funktionale EVG-Sicherheitsanforderungen	
	principal	supporting
O.InformationFlow	FDP_IFC.1, FDP_IFF.1, FDP_ETC.1, FDP_ITC.1	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1A, FMT_MTD.3, FMT_SMR.2, FIA_UID.2, FIA_UID.2A, FPT_ITT.1, FPT_RVM.1, FPT_SEP.1, AVA_MSU.3
O.Disclosure	FDP_IFC.1, FDP_IFF.1, FDP_ETC.1, FDP_ITC.1	FMT_MTD.1A, FMT_MTD.3, FCS_COP.1A – FCS_COP.1C, AVA_MSU.3
O.Manipulation	FDP_IFC.1, FDP_IFF.1, FDP_ETC.1, FDP_ITC.1	FMT_MTD.1A, FMT_MTD.3, FCS_COP.1D – FCS_COP.1F, AVA_MSU.3
O.Support	FDP_IFC.1, FDP_IFF.1, FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FMT_MSA.3, FMT_MTD.3, FMT_SMF.1	FAU_STG.1, FAU_STG.3, FMT_MSA.1, FMT_MTD.1A, FMT_MTD.1B, FPT_STM.1, FIA_UID.2A, FPT_ITT.1, AVA_MSU.3
O.EVG-Administration	FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FIA_UAU.1, FIA_UID.1, FTA_SSL.3, FMT_MOF.1, FMT_MSA.1, FMT_SMR.2, FMT_MTD.1A, FMT_MTD.1B	FPT_RVM.1, FPT_SEP.1, FIA_UAU.2A, FIA_UID.2A, FPT_ITT.1
O.Impersonate	FIA_UAU.1, FIA_UID.1, FTA_SSL.3, FIA_UID.2, FMT_SMR.2	FIA_UAU.2A, FIA_UID.2A, FPT_ITT.1
OE.Disclosure	FCS_COP.1A – FCS_COP.1C	
OE.Manipulation	FCS_COP.1D – FCS_COP.1F	
OE.NoBypass	FPT_RVM.1, FPT_SEP.1	
OE.Selection	FIA_UAU.2A, FIA_UID.2A, FPT_ITT.1, FPT_STM.1	
OE.I&A	FIA_UAU.2A, FIA_UID.2A	

Tabelle 11: Abdeckung der (IT-)Sicherheitsziele durch Sicherheitsanforderungen

Nachfolgend wird für jedes der in Kap. 4 identifizierten (IT-)Sicherheitsziele erklärt, warum es von den in Tabelle 11 aufgeführten funktionalen Sicherheitsanforderungen erfüllt wird. Für das Sicherheitsziel OE.Qualification wird keine solche Erklärung gegeben, weil es sich dabei um ein Sicherheitsziel für die Umgebung handelt, das nicht auf IT bezogen ist. Den Sicherheitszielen OE.NoCapture und OE.NoVirus sind keine funktionalen Sicherheitsanforderungen zugeordnet, weil solche Anforderungen keinen Beitrag zur Durchsetzung der Sicherheitsziele des TOE (EVG) leisten.

Anwendungsbemerkung 18. Der Nachweis der Erfüllung der Sicherheitsziele OE.Qualification, OE.NoCapture und OE.NoVirus ist vom Hersteller zu erbringen. Sie können durch geeignete Schulungsmaßnahmen sowie durch Umsetzung von Maßnahmen des IT-Grundschutzes durchgesetzt werden.

O.InformationFlow

Die Komponenten FDP_IFC.1, FDP_IFF.1, FDP_ETC.1 und FDP_ITC.1 sichern, dass angeforderte Informationsflüsse innerhalb des IT-Systems und aus dem IT-System heraus bzw. in dieses hinein in Übereinstimmung mit der vermittels der RuleData präzisierten EVG-Sicherheitspolitik kontrolliert werden. Die Komponenten FMT_MTD.1A und FMT_MTD.3 sichern insbesondere die Zuverlässigkeit der RuleData in Bezug auf die Verträglichkeit der formulierten Informationsflussvorschriften.

Die Komponenten FMT_MTD.1A, FMT_MTD.3, FMT_MSA.1 und FMT_MSA.3 sichern die Zuverlässigkeit der Sicherheitsattribute. Die Komponenten FPT_ITT.1, FIA_UID.2, FIA_UID.2A und FMT_SMR.2 sichern die Zuverlässigkeit der Informationen und der Rollenzuweisung, anhand derer gemäß FDP_IFF.1 entschieden wird, ob ein angeforderter Informationsfluss erlaubt ist oder verweigert wird.

Die Komponente FMT_MOF.1 gewährleistet, unterstützt von FPT_RVM.1 und FPT_SEP.1, dass die Funktionen zur Durchsetzung der EVG-Sicherheitspolitik immer aktiv sind und nicht umgangen werden können.

Die Komponente AVA_MSU.3 trägt zur Durchsetzung der EVG-Sicherheitspolitik bei, indem sie den IT-Benutzer und den EVG-Administrator bei der erforderlichen Interaktion (Information über verweigerte Informationsflüsse und daraus abzuleitende Maßnahmen) unterstützt.

O.Disclosure

Die Komponenten FDP_IFC.1, FDP_IFF.1, FDP_ETC.1 und FDP_ITC.1 sichern, dass angeforderte Informationsflüsse innerhalb des IT-Systems und aus dem IT-System heraus bzw. in dieses hinein in Übereinstimmung mit der vermittels der RuleData präzisierten Sicherheitspolitik kontrolliert werden. Die Komponenten FMT_MTD.1A und FMT_MTD.3 sichern insbesondere die Zuverlässigkeit der RuleData in Bezug auf die Verträglichkeit der formulierten Informationsflussvorschriften.

Die von der IT-Umgebung durch die Komponenten FCS_COP.1A – FCS_COP.1C zur Verfügung gestellten Verschlüsselungsverfahren garantieren, dass gemäß FDP_IFF.1 zu berücksichtigende Informationsflussvorschriften, die auf den Schutz der Vertraulichkeit von UserData zielen, korrekt umgesetzt werden.

Die Komponente AVA_MSU.3 trägt zur Durchsetzung der EVG-Sicherheitspolitik bei, indem sie den IT-Benutzer bei der erforderlichen Interaktion (Information über fehlgeschlagene Ver-/Entschlüsselung und daraus abzuleitende Maßnahmen) unterstützt.

Anforderungskomponenten für die vertrauenswürdige Übertragung der UserData zu den kryptographischen Modulen, wie etwa FDP_UCT.1, FDP_UIT.1 und FTP_ITC.1, sind nicht Bestandteil dieses Schutzprofils. Solche Komponenten werden benötigt, wenn der kryptographische Betrieb nicht innerhalb des TOE (EVG) stattfindet (Component TOE (EVG)). Auf ihre Berücksichtigung in diesem Schutzprofil kann jedoch verzichtet werden, weil sie lediglich unterstützend zur Durchsetzung des Sicherheitsziels O.Disclosure beitragen und weil sie bei Integration des kryptographischen Betriebs in den TOE (EVG) dafür nicht erforderlich sind (vgl. Kapitel PP-Anwendungsbemerkungen).

O.Manipulation

Die Komponenten FDP_IFC.1, FDP_IFF.1, FDP_ETC.1 und FDP_ITC.1 sichern, dass angeforderte Informationsflüsse innerhalb des IT-Systems und aus dem IT-System heraus bzw. in dieses hinein in Übereinstimmung mit der vermittels der RuleData präzisierten Sicherheitspolitik kontrolliert werden. Die Komponenten FMT_MTD.1A und FMT_MTD.3 sichern insbesondere die Zuverlässigkeit der RuleData in Bezug auf die Verträglichkeit der formulierten Informationsflussvorschriften.

Die von der IT-Umgebung durch die Komponenten FCS_COP.1D – FCS_COP.1F zur Verfügung gestellten Signierverfahren garantieren, dass gemäß FDP_IFF.1 zu berücksichtigende Informationsflussvorschriften, die auf den Schutz der Integrität und Authentizität von UserData zielen, korrekt umgesetzt werden.

Die Komponente AVA_MSU.3 trägt zur Durchsetzung der EVG-Sicherheitspolitik bei, indem sie den IT-Benutzer bei der erforderlichen Interaktion (Information über fehlgeschlagene Erzeugung/Prüfung elektronischer Signaturen/Zertifikate und daraus abzuleitende Maßnahmen) unterstützt.

Anforderungskomponenten für die vertrauenswürdige Übertragung der UserData zu den kryptographischen Modulen, wie etwa FDP_UCT.1, FDP_UIT.1 und FTP_ITC.1, sind nicht Bestandteil dieses Schutzprofils. Solche Komponenten werden zwar benötigt, wenn der kryptographische Betrieb nicht innerhalb des TOE (EVG) stattfindet (Component TOE (EVG)). Auf ihre Berücksichtigung in diesem Schutzprofil kann jedoch verzichtet werden, weil sie lediglich unterstützend zur Durchsetzung des Sicherheitsziels O.Manipulation beitragen und weil sie bei Integration des kryptographischen Betriebs in den TOE (EVG) dafür nicht erforderlich sind (vgl. Kapitel PP-Anwendungsbemerkungen).

O.Support

Die Komponenten FDP_IFC.1, FDP_IFF.1, FAU_GEN.1, FAU_GEN.2, FAU_SEL.1 stellen sicher, dass Entscheidungen über angeforderte Informationsflüsse in Übereinstimmung mit den in den RuleData getroffenen Festlegungen protokolliert werden. Die für FAU_GEN.2 benötigte Benutzeridentität wird durch die von der Umgebung zur Verfügung gestellte Komponente FIA_UID.2A bereitgestellt; die Komponente FPT_ITT.1 gewährleistet ihre geschützte Übertragung zum TOE (EVG).

FAU_SAR.1 und FAU_SAR.3 garantieren, dass der EVG-Administrator die ProtocolData geeignet analysieren kann, um darauf aufbauend die RuleData zu validieren. Von der Komponente FPT_STM.1 werden die für die Analyse notwendigen zeitlichen Informationen bereitgestellt, deren geschützte Übertragung zum TOE (EVG) von der Komponente FPT_ITT.1 gewährleistet wird. FAU_STG.1, FAU.STG.3 und FMT_MTD.1B gewährleisten die Integrität der einer solchen Analyse und Validierung zugrunde liegenden ProtocolData.

FMT_MSA.3, FMT_MTD.3 und FMT_SMF.1 leisten einen entscheidenden Beitrag, um dem EVG-Administrator die Administration der RuleData zu vereinfachen, indem bspw. das Einstellen von inkonsistenten Listen von Informationsflussregeln verhindert und die Möglichkeiten zur Wiederverwendung bewährter Lösungen angeboten wird. Die Komponente AVA_MSU.3 gewährleistet die Güte der von FMT_SMF.1 geforderten Managementfunktionen.

FMT_MSA.1 und FMT_MTD.1A unterstützen den EVG-Administrator, indem sie dazu beitragen zu sichern, dass die für die Politikentscheidungen wichtigen RuleData und Sicherheitsattribute nicht ohne sein Wissen verändert werden können.

O.EVG-Administration

Durch das Zusammenspiel der Komponenten FIA_UID.1, FIA_UAU.1, FTA_SSL.3, FMT_SMR.2, FAU_SAR.1, FAU_SAR.2 und FMT_MTD.1B, unterstützt von FPT_SEP.1, wird garantiert, dass nur ein in der Rolle EVG-Administrator agierender Benutzer von den ProtocolData Kenntnis nehmen kann. FAU_SAR.1 und FAU_SAR.3 bewirken, dass der EVG-Administrator die ProtocolData geeignet analysieren kann.

Die Komponenten FIA_UID.1, FIA_UAU.1, FTA_SSL.3, FMT_SMR.2 und FMT_MOF.1 stellen sicher, dass nur der EVG-Administrator den TOE (EVG) deaktivieren kann. Die von der Umgebung bereitgestellten Komponenten FPT_SEP.1 und FPT_RVM.1 unterstützen dieses.

Die Komponenten FIA_UID.1, FIA_UAU.1, FTA_SSL.3, FMT_SMR.2, FMT_MSA.1 und FMT_MTD.1A, unterstützt von FPT_SEP.1, sichern, dass die für die Politikentscheidungen wichtigen RuleData und Sicherheitsattribute nur von der Rolle des EVG-Administrator verändert werden.

Unterstützend für die Rollenzuweisung dienen die von der Umgebung bereitgestellten Komponenten FIA_UAU.2A und FIA_UID.2A. Die Komponente FPT_ITT.1 gewährleistet die geschützte Übertragung der Benutzerkennung zum TOE (EVG).

O.Impersonate

Durch die Komponenten FIA_UID.1, FIA_UAU.1, FTA_SSL.3 und FMT_SMR.2 ist sichergestellt, dass nur berechtigte Personen in der Rolle EVG-Administrator agieren können. Die Korrektheit der Rollenzuweisung für IT-Benutzer und IT-Administrator wird durch die Komponenten FIA_UID.2 und FMT_SMR.2 gewährleistet. Die Komponente FMT_SMR.2 stellt sicher, dass die Rolle IT-Administrator und eine der Rollen IT-Benutzer bzw. EVG-Administrator nicht gleichzeitig agieren können.

Unterstützend für die Rollenzuweisung dienen die von der Umgebung bereitgestellten Komponenten FIA_UAU.2A und FIA_UID.2A. Die Komponente FPT_ITT.1 gewährleistet die geschützte Übertragung der Benutzerkennung zum TOE (EVG).

OE.Disclosure

Die IT-Umgebung stellt gemäß FCS_COP.1A – FCS_COP.1C geeignete kryptographische Funktionen (speziell: Verschlüsselungsverfahren) zur Verfügung, mit denen UserData derart verschlüsselt werden können, dass sie sowohl innerhalb des IT-Systems als auch während der Übertragung vor unberechtigter Kenntnisnahme gesichert sind.

OE.Manipulation

Die IT-Umgebung stellt gemäß FCS_COP.1D – FCS_COP.1F geeignete Hashverfahren, Verfahren zum Erzeugen elektronischer Signieren und Verfahren zum Prüfen von elektronischen Signaturen und Zertifikaten zur Verfügung. Eine geeignete Anwendung von Hashverfahren und Verfahren zum Erzeugen elektronischer Signaturen macht es möglich, UserData innerhalb des IT-Systems bzw. während der Übertragung vor unbemerkter Modifikation zu schützen und Authentizitätsnachweise anzubringen. Die Verfahren zum Prüfen von elektronischen Signaturen und Zertifikaten können eingesetzt werden, um die Integrität und Authentizität von UserData zu verifizieren.

OE.NoByPass

Durch die Komponente FPT_RVM.1 ist gewährleistet, dass der TOE (EVG) immer aktiv ist. Die Komponente FPT_SEP.1 gestattet es, die TSF-Data derart zu schützen, dass der TOE (EVG) wie beabsichtigt arbeitet. Folglich ist gesichert, dass alle Informationsflüsse vom TOE (EVG) kontrolliert werden.

OE.Selection

Die Komponenten FPT_STM.1 bzw. FIA_UID.2A und FIA_UAU.2A sichern, dass die von der IT-Umgebung zur Verfügung gestellten Zeitstempel bzw. Benutzerauthentisierungen und Benutzeridentifikationen verlässlich sind und auch von seiten eines IT-Administrators (der als potenzieller Angreifer zu sehen ist) nicht überwunden werden können. Die Komponente FPT_ITT.1 garantiert, dass diese und alle übrigen Informationen zur Identifikation angeforderter Informationsflüsse gegen Modifikation geschützt zum TOE (EVG) übertragen werden. Damit kann gewährleistet werden, dass die bereitgestellten Informationen korrekt sind.

OE.I&A

Die Komponenten FIA_UAU.2A und FIA_UID.2A sichern, dass das IT-System erst nach erfolgreicher Identifikation und Authentisierung benutzt werden kann.

7.2.2 Abhängigkeiten der funktionalen Sicherheitsanforderungen

Tabelle 12 gibt eine Übersicht über die funktionalen Sicherheitsanforderungen dieses Schutzprofils und ihrer Abhängigkeiten. Für jede Abhängigkeit ist angegeben, ob und durch welche andere funktionale Anforderung dieses Schutzprofils sie aufgelöst wird. Es sei angemerkt, dass die Abhängigkeiten von FCS_COP.1A – FCS_COP.1F auf FDP_ITC.1 und FCS_CKM.1 alternativ zu erfüllen sind. Bei allen anderen alternativen Abhängigkeiten sind nur die jeweils ausgewählten Alternativen angegeben.

Die Abhängigkeiten sind für alle Komponenten mit Ausnahme für FMT_MTD.3 und FCS_COP.1A – FCS_COP.1F aufgelöst.

FMT_MTD.3

Die Abhängigkeit von ADV_SPM.1 ist nicht aufgelöst worden, weil durch das Verfeinerungselement FMT_MTD.3.a eine klare Definition der sicheren Werte gegeben ist. Die Begründung für diese Definition ergibt sich direkt aus der Spezifikation der EVG-Sicherheitspolitik (vgl. Kap. 2.5). Gemäß Common Criteria[106] kann daher die Abhängigkeit entfallen.

FCS_COP.1A – FCS_COP.1F

Die Abhängigkeiten für FCS_COP.1A – FCS_COP.1F sind nicht aufgelöst worden, weil für die Realisierung des kryptographischen Betriebs eine Vielzahl von möglichen Alternativen besteht. Es ist daher nicht zweckmäßig, in diesem Schutzprofil detaillierte Anforderungen an die Kombination des kryptographischen Betriebs mit der spezifizierten Sicherheitspolitik zu stellen. Die offenen Abhängigkeiten für FCS_COP.1 verpflichten den ST-Autor, solche Anforderungen zu ergänzen. Dies betrifft insbesondere den wichtigen Bereich des Managements der kryptographischen Schlüssel (Familie FMT_CKM).

[106] Zitat aus Common Criteria, Teil 2, Anhang H.3, Absatz 1046: „Wenn der Entwickler eine klare Definition der sicheren Werte und den Grund, warum diese als sicher angesehen werden können, bereitgestellt hat, kann die Abhängigkeit für FMT_MTD.3 von ADV_SPM.1 begründet entfallen.“

Nr.	CC-Komponente	Abhängigkeit	Aufgelöst durch
1.	FAU_GEN.1	FPT_STM.1	Nr. 30
2.	FAU_GEN.2	FAU_GEN.1 FAU_UID.1	Nr. 1 Nr. 26
3.	FAU_SAR.1	FAU_GEN.1	Nr. 1
4.	FAU_SAR.2	FAU_SAR.1	Nr. 3
5.	FAU_SAR.3	FAU_SAR.1	Nr. 3
6.	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Nr. 1 Nr. 19b
7.	FAU_STG.1	FAU_GEN.1	Nr. 1
8.	FAU_STG.3	FAU_STG.1	Nr. 7
9.	FDP_ETC.1	FDP_IFC.1	Nr. 10
10.	FDP_IFC.1	FDP_IFF.1	Nr. 11
11.	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Nr. 10 Nr. 18
12.	FDP_ITC.1	FDP_IFC.1 FMT_MSA.3	Nr. 10 Nr. 18
13.	FIA_UAU.1	FIA_UID.1	Nr. 14
14.	FIA_UID.1	keine	—
15.	FIA_UID.2	keine	—
16.	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Nr. 21 Nr. 22
17.	FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Nr. 10 Nr. 22 Nr. 21
18.	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Nr. 17 Nr. 22
19a.	FMT_MTD.1A	FMT_SMF.1 FMT_SMR.1	Nr. 21 Nr. 22
19b.	FMT_MTD.1B		
20.	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	nicht aufgelöst Nr. 19a
21.	FMT_SMF.1	keine	—
22.	FMT_SMR.2	FIA_UID.1	Nr. 14 (EVG-Administrator) Nr. 15 + 26 (IT-Benutzer, IT-Administrator)
23.	FTA_SSL.3	keine	—
24.	FCS_COP.1A – FCS_COP.1F	FDP_ITC.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	nicht aufgelöst nicht aufgelöst nicht aufgelöst nicht aufgelöst
25.	FIA_UAU.2A	FIA_UID.1	Nr. 26
26.	FIA_UID.2A	keine	—
27.	FPT_RVM.1	keine	—
28.	FPT_ITT.1	keine	—
29.	FPT_SEP.1	keine	—
30.	FPT_STM.1	keine	—

Tabelle 12: Abhängigkeiten zwischen den funktionalen Sicherheitsanforderungen

7.2.3 Gegenseitige Unterstützung der funktionalen Sicherheitsanforderungen

In Abschnitt 7.2.1 wird der Schutz der als „principal“ klassifizierten funktionalen Sicherheitsanforderungen durch unterstützende („supporting“) funktionale Sicherheitsanforderungen erläutert. Insbesondere wird die Durchsetzung der SFP der benutzerbestimmbaren Informationsflusskontrolle unterstützt

- durch die von der Komponente FMT_MOF.1 geforderte Beschränkung der Deaktivierung des TOE (EVG) auf den EVG-Administrator.
- durch den von der Komponente FPT_RVM.1 geforderten Schutz gegen Umgehung des aktiven TOE (EVG), der durch die IT-Umgebung zu gewährleisten ist.
- durch den von der Komponente FPT_SEP.1 geforderten Schutz gegen Manipulation des TOE (EVG), der durch die IT-Umgebung zu gewährleisten ist.

Die Komponente FMT_MOF.1 unterstützt die Komponenten FDP_IFC.1 und FDP_IFF.1. Die Komponenten FPT_RVM.1 und FPT_SEP.1 leisten einen Beitrag zur Unterstützung der Komponenten FDP_IFC.1, FDP_IFF.1, FIA_UAU.1, FIA_UID.1 FTA_SSL.3 und FMT_MOF.1. Darüber hinaus dient FPT_SEP.1 zur Unterstützung der Komponenten FAU_SAR.1, FAU_SAR.2, FMT_MSA.1, FMT_MTD.1A und FMT_MTD.1B.

Weiterhin ist in Abschnitt 7.2.1 die Weglassung von unterstützenden CC-Komponenten für die Formulierung von Anforderungen an einen vertrauenswürdigen Kanal zum Datenaustausch mit externen kyptographischen Modulen (vgl. O.Disclosure bzw. O.Manipulation sowie Kap. 6) begründet.

In Abschnitt 7.2.2 werden die Abhängigkeiten der funktionalen Komponenten untersucht und nicht aufgelöste Abhängigkeiten begründet.

Zusätzlich wird hier erklärt, dass die durchgeführten Operationen miteinander abgestimmt sind.

Auswahloperationen
Alle Auswahloperationen, insbesondere die Wahl des Protokollierungsgrades „Minimal“ (FAU_GEN.1) und die Wahl von Standardwerten für Sicherheitsattribute mit „freizügigen“ Eigenschaften (FMT_MSA.3), sind miteinander abgestimmt und stimmen mit dem angenommenen geringen Bedrohungspotential überein.

Zuweisungsoperationen
Alle Zuweisungsoperationen, insbesondere die Festlegung der durchzusetzenden Sicherheitspolitik (FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FIA_UAU.1, FIA_UID.1, FMT_MSA.1, FMT_MSA.3 und FMT_SMF.1), sind miteinander und mit den Bedingungen für die Rollenzuweisung (FIA_UAU.1, FIA_UAU.2A, FIA_UID.1, FIA_UID.2, FIA_UID.2A und FMT_SMR.2) abgestimmt und spezifizieren ganzheitlich eine in sich konsistente Sicherheitsleistung.

Iterationsoperationen
Die Iteration der Komponente FMT_MTD.1 ist notwendig zur Unterscheidung der RuleData von den ProtocolData. Die iterierten Komponenten werden auf konsistente Weise zur Auflösung der Abhängigkeiten verwendet (s. Kap. 7.2.2).
Die gleichzeitige Verwendung der hierarchischen Komponenten FIA_UID.1 und FIA_UID.2 im TOE (EVG) ist notwendig, da sie zur Zuweisung unterschiedlicher Rollen mit unterschiedlichen Befugnissen verwendet werden. Die gleichzeitige Verwendung der hierarchischen Komponenten FIA_UAU.1 und FIA_UAU.2A bzw. FIA_UID.1 und FIA_UID.2A ist notwendig, da sowohl eine Identifizierung und Authentisierung der rechtmäßigen Benutzer durch die IT-Umgebung (FIA_UAU.2A und FIA_UID.2A) als auch eine Identifikation und Authentisierung der Rolle EVG-Administrator (FIA_UAU.1 und FIA_UID.1) seitens des TOE (EVG) gefordert wird. Die Komponenten der Familie FIA_UID werden auf konsistente Weise zur Auflösung der Abhängigkeiten von FMT_SMR.2 verwendet (s. Kap. 7.2.2 und Kap. 5.1.1.3).
Die Iteration der Komponente FCS_COP.1 ist notwendig zur Unterscheidung der verschiedenen kryptographischen Algorithmen.

Verfeinerungsoperationen
Alle Verfeinerungsoperationen sind abgestimmt mit

- der Verwendung der Komponenten für die IT-Umgebung (s. Abschnitt 5.2) und
- den komplexen Managementanforderungen für die durchzusetzende Sicherheitspolitik (s. Klassen FIA und FMT).

7.2.4 Erklärung der Anforderungen an die Vertrauenswürdigkeit

Die Anforderungen an die Vertrauenswürdigkeit gemäß der gewählten Evaluierungsstufe EAL 2 sind angemessen für den TOE (EVG), weil davon ausgegangen wird, dass die Sicherheitsleistung höchstens gegen offensichtliche Penetrationsangriffe schützen soll.
Die Augmentierung mit der Komponente AVA_MSU.3 ermöglicht die Bewertung der besonderen Anforderungen an die Administration des TOE (EVG) (vgl. Verfeinerung der Komponente FMT_SMF.1).
Durch die Wahl der vorgegebenen Evaluierungsstufe EAL 2 ist die Auflösung der Abhängigkeiten der Anforderungen an die Vertrauenswürdigkeit automatisch gegeben. Für die Komponente AVA_MSU.3 sind keine zusätzlichen Abhängigkeiten gefordert.

7.2.5 Erklärung der Mindest-Stärkestufe der Funktionen

Nach dem Stand der Kunst stehen Mechanismen im Bereich Kryptographie und Authentisierung zur Verfügung, die die Stärkestufe SOF-Mittel erreichen. Obwohl die Sicherheitsleistung des TOE (EVG) höchstens gegen offensichtliche Penetrationsangriffe schützen soll, muss insbesondere berücksichtigt werden, dass verschlüsselte und/oder signierte Datenbestände über lange Zeiträume aufbewahrt werden. Das Postulat SOF-Mittel für die Mindest-Stärkestufe der Funktionen ist unter Berücksichtigung der dauerhaften Aufrechterhaltung des Schutzes von Informationen angemessen für den TOE (EVG).

A Glossar

Applikation Ein Anwendungsprogramm, dem Prozesse auf Betriebssystemebene zugeordnet werden können. Beispiel für eine aktive funktionale Einheit als Teil eines *Subjekts*.

Auswahlfunktion Funktion, die aus einer Liste von *Informationsflussregeln* diejenige auswählt, anhand derer entschieden wird, ob der Informationsfluss erlaubt oder verweigert wird.

Betriebssystem Der Teil eines *IT-Systems*, welcher die Ressourcenverwaltung übernimmt.

Datenort Die eindeutige Beschreibung für einen Ort, an dem sich eine passive Einheit (ein *Objekt*) befindet. Die Ortsangabe kann sich auf ein auf einem lokalen Speichermedium befindliches *Objekt* oder auf ein über eine Netzverbindung erreichbares *Objekt* beziehen.

Deaktivieren des TOE (EVG) Der *TOE (EVG)* gilt als deaktiviert, wenn er außerstande gesetzt wird, stattfindende *Informationsflüsse* in Bezug auf die festgelegten *Informationsflussregeln* zu kontrollieren. Da der *TOE (EVG)* transparent arbeitet, sollte auch seine Deaktivierung für den Benutzer transparent sein. Das bedeutet, dass ein Benutzer von der Deaktivierung (genauso wie von der Aktivierung) des *TOE (EVG)* nichts bemerken sollte, was wiederum zur Folge hat, dass z.B. durch den *TOE (EVG)* verschlüsselte Daten bei der Deaktivierung wieder zu entschlüsseln sind. Insbesondere handelt es sich also beim Löschen des *TOE (EVG)*-Programmcodes nicht um eine Deaktivierung, da in diesem Fall die Verschlüsselungen erhalten bleiben. Des Weiteren bedeutet dies, dass eine Deinstallation des *TOE (EVG)* eine vorher durchzuführende Deaktivierung einschließen sollte.

EVG-Administrator Rolle, die zur Administration des *TOE (EVG)* und zum Lesen der *ProtocolData* berechtigt.

EVG-Sicherheitspolitik Die Gesamtheit der *Funktionalen Sicherheitspolitiken* definiert die EVG-Sicherheitspolitik.

Flag Binäres Attribut, das den Wert „True“ oder „False“ annehmen kann.

Funktionale Sicherheitspolitik Eine Teilmenge der *EVG-Sicherheitspolitik*, die innerhalb ihres Anwendungsbereichs die zu kontrollierenden *Objekte/Informationen*, *Subjekte* und Operationen festlegt.

Informationen Mit *Objekten* verknüpfte Daten.

Informationsfluss Ein Fluss von *Informationen* als Folge einer durch ein *Subjekt* ausgelösten Operation. Betrachtete Operationen sind das Lesen oder Schreiben von *Informationen* aus/in *Objekten.*

Informationsflussregel Regeln, auf Basis derer durch den *TOE (EVG)* entschieden wird, ob ein angeforderter *Informationsfluss* zu erlauben bzw. zu verweigern ist. Sie legen u.a. fest, welche *Subjekte Informationen* in *Objekte* an *kontrollierten Datenorten* schreiben bzw. *Informationen* aus *Objekten* an *kontrollierten Datenorten* lesen dürfen und welche *Informationsflussvorschriften* bei einem *Informationsfluss* zu berücksichtigen sind.

Informationsflussvorschrift Vorschrift, die die Art und die Reihenfolge der Operationen festlegt, die auszuführen sind, bevor *Information* aus einem *Objekt* gelesen bzw. in ein *Objekt* geschrieben wird.

IT-Administrator Rolle, die zum Administrieren des *IT-Systems* und zum Installieren des *TOE (EVG)* berechtigt.

IT-Benutzer Rolle, die zum Benutzen des *IT-Systems* berechtigt.

IT-System Das Gesamtsystem, bestehend aus Hard- und Softwarekomponenten, auf dem der *TOE (EVG)* installiert ist und auf dem die *EVG-Sicherheitspolitik* durchgesetzt werden soll.

Kontrollierter Datenort Datenort, für den es eine *spezifischste Informationsflussregel* gibt, in der das Kontrollflag gesetzt ist.

Konsistente Liste von Informationsflussregeln Liste von *Informationsflussregeln*, mit speziellen Eigenschaften, die u.a. garantieren, dass es zu jedem *Datenort* nur eine *spezifischste Informationsflussregel* gibt und dass *Informationsflussvorschriften* einander nicht widersprechen.

Objekte Passive Einheiten, die *Informationen* enthalten können und Ziel von Operationen sind, die von *Subjekten* ausgeführt werden.

ProtocolData Die ProtocolData umfassen alle vom *TOE (EVG)* protokollierten Ereignisse. Hierzu gehören insbesondere erlaubte und verweigerte *Informationsflüsse*.

Rolle Definiert die erlaubten Tätigkeiten einer Klasse von Benutzern des *TOE (EVG)*, wobei ein Benutzer gleichzeitig mehrere (im Extremfall sogar alle) Rollen innehaben kann.

RuleData Teil der *TSF-Data*, welcher die Liste der eingestellten *Informationsflussregeln* umfasst.

Sicherheitsattribut Attribute, die *Subjekten, Informationen* und/oder *Objekten* zugeordnet werden, um eine *Funktionale Sicherheitspolitik* zu definieren.

Spezifischste Informationsflussregel *Informationsflussregel* R, in der der betreffende *Datenort* genannt wird und für die gilt, dass es keine *Informationsflussregel* gibt, in der neben diesem *Datenort* nur einige der in R genannten *Datenorte* genannt werden.

Subjekte Paare aus Benutzerkennung und weiteren Angaben, die zur Beschreibung der aktiven Einheit (bspw. *Applikationen* zugeordnete Prozesse) innerhalb des *TOE (EVG)* benötigt werden.

TOE (EVG) Evaluationsgegenstand – im vorliegenden Fall ein Sicherheitsprodukt, das sowohl als reine Softwarelösung als auch als Kombination aus Hard- und Softwarekomponenten realisiert sein kann.

Trojaner Eine böswilliges Programm, welches sich als gutartig tarnt, um vom *IT-Benutzer* unbemerkt Schaden am *IT-System* anzurichten.

TSF-Data Daten, die für Entscheidungen im Rahmen der *EVG-Sicherheitspolitik* benutzt werden. Hierzu gehören u.a. *ProtocolData* und *RuleData*.

Unautorisierter Benutzer Benutzer des *IT-Systems*, die nicht dazu berechtigt sind, in einer der Rollen *IT-Benutzer*, *IT-Administrator* bzw. *EVG-Administrator* zu agieren.

UserData *Informationen*, mit denen die Benutzer Operationen ausführen können und die nicht für Entscheidungen im Rahmen der *EVG-Sicherheitspolitik* benutzt werden. Es handelt sich um *Informationen*, die von einem *IT-Benutzer* im Rahmen seiner Tätigkeit verarbeitet werden.

Wartung Alle Arbeiten an einem *IT-System*, die die bestimmungsgemäße Funktion des *IT-Systems* sicherstellen.

B Abkürzungen

ANSI	American National Standards Institute
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
E-	Electronic-
EVG	Evaluierungsgegenstand
FIPS	Federal Information Processing Standards
IEC	International Electrotechnical Commision
ISO	International Organisation for Standardization
IT	Information Technology
LAN	Local Area Network
MU	Multi-user
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
SFP	Security Functional Policy
ST	Security Target
SU	Single-user
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WAN	Wide Area Network

C Literatur

[BISS-SU] Bundesamt für Sicherheit in der Informationstechnik (BSI). Benutzerbestimmbare Informationsflusskontrolle (SU). Common Criteria Schutzprofil BSI-PP-0007, Version 2.01, 4. September 2002.

[FIPS 46-3] FIPS Publication 46-3. Data Encryption Standard (DES). October 25, 1999.

[FIPS 81] FIPS Publication 81. DES Modes of Operation. December 2, 1980.

[FIPS 180-1] FIPS Publication 180-1. Secure Hash Standard (SHS). April 17, 1995.

[FIPS 197] FIPS Publication 197. Advanced Encryption Standard (AES). November 26, 2001.

[ISO/IEC 10116] ISO/IEC 10116:1997. Modes of Operation for an n-bit block cipher algorithm. 1997.

[PKCS #1] RSA Laboratories. PKCS #1 v.2.0: RSA Cryptography Standard. October 1998.

[SPHINX] Bundesamt für Sicherheit in der Informationstechnik (BSI). SPHINX Pilotversuch Ende-zu-Ende-Sicherheit: Technische Grundlagen – Tailoring MTTv2. Version 2.0, 15. August 2000.

[X9.52] ANSI X9.52-1998. Triple Data Encryption Algorithm Modes of Operation.