Schutzprofil SIZ-PP

Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister

Version 2.0

Februar 2000

Inhaltsverzeichnis

1 Einleitung 5

1.1 Allgemeine Hinweise 5

1.2 Zielgruppen 5

1.3 Terminologie 6

1.3.1 Abkürzungen 6

1.3.2 Glossar 7

1.4 Bezüge zu anderen Arbeiten 8

1.5 Literaturverzeichnis 9

2 Schutzprofil 10

2.1 Bezeichnung 10

2.2 Überblick und Abgrenzung 10

2.3 Stärke der Sicherheitsfunktionen 11

3 Beschreibung des EVG 12

4 Sicherheitsumgebung 13

4.1 Annahmen zum sicheren Betrieb 13

4.1.1 Annahmen zur Betriebsumgebung 13

4.1.2 Annahmen zum Bedienungspersonal 13

4.1.3 Annahmen zu Kommunikationsverbindungen 13

4.1.4 Annahmen zur organisatorischen Umgebung 14

4.2 Bedrohungen 15

4.2.1 Vom EVG abzuwehrende Bedrohungen 15

4.2.2 Von der Betriebsumgebung abzuwehrende Bedrohungen 17

4.3 Organisatorische Sicherheitspolitiken 19

4.3.1 Grundsätze der IT-Sicherheitspolitik (Sicherheitsgrundsätze) 19

4.3.2 Sicherheitsstrategien / Sicherheitspolitiken 20

5 Sicherheitsziele 28

5.1 Sicherheitsziele für den EVG 28

5.2 Sicherheitsziele für die Umgebung 29

6 IT-Sicherheitsanforderungen 31

6.1 Funktionale Sicherheitsanforderungen an den EVG 31

6.1.1 Tabellarische Übersicht 31

6.1.2 Identifikation und Authentisierung (FIA) 33

6.1.3 EVG-Zugriff (FTA) 39
6.1.4 Schutz der Benutzerdaten (FDP) 42
6.1.5 Schutz der EVG-Sicherheitsfunktionen (FPT) 48
6.1.6 Kommunikation (FCO) 54
6.1.7 Vertrauenswürdiger Pfad/Kanal (FTP) 56
6.1.8 Kryptographische Unterstützung (FCS) 58
6.1.9 Sicherheitsprotokollierung (FAU) 60
6.1.10 Sicherheitsmanagement (FMT) 69

6.2 Anforderungen zur Vertrauenswürdigkeit 80
6.2.1 Interna der EVG-Sicherheitsfunktionen (ADV_INT) 80
6.2.2 Fehlerbehebung (ALC_FLR) 80

6.3 Sicherheitsanforderungen an die IT-Umgebung 81

7 Anwendungshinweise zum Schutzprofil 82

8 Erklärungen 83

8.1 Einleitung 83

8.2 Erklärungen der Sicherheitsziele 83
8.2.1 Bedrohungen und Sicherheitsziele 83
8.2.2 Abdeckung der Sicherheitspolitik durch die Sicherheitsziele 89
8.2.3 Bezug zwischen Sicherheitszielen und Annahmen 98
8.2.4 Vollständigkeit der Abdeckung 98

8.3 Erklärungen der Sicherheitsanforderungen 100
8.3.1 Sicherheitsziele und Sicherheitsanforderungen 100
8.3.2 Abdeckung der Sicherheitsziele durch die Sicherheitsfunktionen 108

8.4 Erklärung zur Auswahl der Anforderungen an die Vertrauenswürdigkeit ... 117
8.4.1 Vertrauenswürdigkeitsstufe 4 (EAL4) – methodisch entwickelt, getestet und durchgesehen 117
ADV_INT.1 Modularität 117
ALC_FLR.3 – Systematische Fehlerbehebung 118

8.5 Konsistenz der Sicherheitsanforderungen 118

1 Einleitung

1.1 Allgemeine Hinweise

Die angestrebte Vereinheitlichung der Datenverarbeitung in der Sparkassenorganisation und der hierzu eingeschlagene Weg einer einheitlichen, kooperativen Anwendungsentwicklung für eine verteilte und für den Anwender transparente Systemumgebung erfordern einheitliche Standards der Sicherheit in der Informationstechnik (IT) sowohl für die Gesamtheit als auch für die einzelnen Komponenten der Anwendungssysteme der Sparkassenorganisation.

Jedes Computersystem, das an ein Rechenzentrum oder verteiltes Netzwerk angeschlossen ist, soll Sicherheitsleistungen enthalten, die einem akzeptierten Sicherheitsstandard entsprechen oder darüber hinausgehen. Solche Sicherheitsleistungen werden nicht nur für die Sicherheitsmechanismen der Anwendungsprogramme bereitgestellt, sondern überwachen auch die Sicherheit der Programme selber und der dazugehörigen Dateien und Transaktionen.

Das hier vorgelegte Schutzprofil SIZ-PP „Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister" zur Anwendung im Rahmen der Common Criteria[1] [CC] wurde mit der Zielsetzung erstellt, grundlegende Sicherheitsanforderungen für

- die Entwicklung,
- den Betrieb und
- die Beschaffung

aller IT-Systeme bei der Sparkassenorganisation zu definieren.

1.2 Zielgruppen

Entsprechend der oben formulierten Ziele wendet sich dieses Schutzprofil an verschiedene Zielgruppen:

Mitglieder der Sparkassenorganisation

Die Mitglieder der Sparkassenorganisation können mit diesem Schutzprofil vorhandene IT-Systeme bezüglich ihrer Sicherheit bewerten, sowie Vorgaben für die Entwicklung, den Betrieb und die Beschaffung von IT-Systemen definieren.

Hersteller

Hersteller können anhand des Schutzprofiles ihre eigenen IT-Produkte bewerten und damit erkennen, wie sie ihre Produkte den Sicherheitserfordernissen der Sparkassenorganisation optimal anpassen können.

Öffentlichkeit

Das SIZ und die Mitglieder der Sparkassenorganisation verstehen das Schutzprofil als Bestandteil eines offenen Prozesses, bei dem Entschei-

[1] vgl. Abschnitt 1.3 „Terminologie"

dungen zur IT-Sicherheit soweit wie möglich einer öffentlichen Begutachtung zugänglich gemacht werden. Dies soll den Kunden der Sparkassenorganisation zeigen, welche Anstrengungen im Bereich der IT-Sicherheit unternommen werden. Gleichzeitig wird dadurch die Möglichkeit eines Feedbacks gegeben, so daß Anregungen in der Fortschreibung des Standards möglicherweise berücksichtigt werden können.

1.3 Terminologie

Dieses Dokument benutzt die Terminologie der im Vorfeld der internationalen Norm ISO/IEC 15408 „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ veröffentlichten „Common Criteria for Information Technology Security Evaluation“ [CC] in der Version 2.1 und deren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellten deutschsprachigen Übersetzung. Aus Gründen der Übersichtlichkeit wird der Begriff „Common Criteria“ in diesem Dokument als einheitliche Bezeichnung für diese Referenzdokumente verwendet.

Da dieses Schutzprofil Gesamtsysteme beschreibt, wurde der sonst übliche Begriff des Evaluationsgegenstandes (EVG) oft durch den Begriff „System“ (eigentlich IT-System) ersetzt. die beiden Begriffe können in diesem Schutzprofil austauschbar verwendet werden.

1.3.1 Abkürzungen

ACL	Zugriffskontrolliste (Access Control List)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for Information Technology Security Evaluation
DAC	benutzerbestimmte Zugriffskontrolle (Discretionary Access Control)
EAL	Vertrauenswürdigkeitsstufe (Evaluation Assurance Level)
EVG	Evaluationsgegenstand (TOE – Target of Evaluation)
IT	Informationstechnik
PC	Arbeitsplatzrechner (Personal Computer)
PIN	Geheimzahl (Personal Identification Number)
PP	Schutzprofil (Protection Profile)
RBAC	rollenbasierte Zugriffskontrolle (Role Based Access Control)
SF	Sicherheitsfunktion, Sicherheitsfunktionen (Security Function)
SFP	Funktionale Sicherheitspolitik (Security Function Policy)
SIZ	Informatikzentrum der Sparkassenorganisation GmbH
SoF	Stärke der Funktionen (Strength of Function)
ST	Sicherheitsvorgaben (Security Target)
SW	Software
TSC	Anwendungsbereich der TSF-Kontrolle (TSF Scope of Control)
TSF	EVG-Sicherheitsfunktionen (TOE Security Functions)
TSP	EVG-Sicherheitspolitik (TOE Security Policy)
ZKA	Zentraler Kreditausschuß

1.3.2 Glossar

In diesem Glossar werden Begriffe, die im Schutzprofil benutzt werden, erläutert. Begriffe, die konform zu den Common Criteria verwendet werden, sind in [CC] definiert.

Benutzer	Nutzer von IT-Systemen oder IT-Dienstleistungen auf den betrachteten IT-Systemen. (Siehe auf Rollenfestlegungen in FMT_SMR.2.1 S.77)
Einfache Benutzer	Benutzer ohne administrative Privilegien.
Kunden	Je nach Kontext Endkunden der Sparkassen oder die Kunden der Entwicklungseinheiten der Sparkassenorganisation, d.h. Sparkassen selbst, die bei diesen Entwicklungseinheiten IT-Dienstleistungen beziehen.
Mitarbeiter	Beschäftigter der Sparkasse oder Entwicklungseinheit.
Partner	Externe Personen oder Organisationen, die in Kooperation mit Sparkassen oder Entwicklungseinheiten IT-Dienstleistungen anbieten oder verwirklichen.
Beweispflicht	Pflicht der Bank, über vollzogene Transaktionen Daten zum Nachweis der Ordnungsmäßigkeit und zur Nachvollziehbarkeit zu sammeln und aufzubewahren.
Credential	Übersetzt: Ausweispapier. Eine Sammlung von Daten, die ein Subjekt einem anderen Subjekt vorlegt, um seine Identität zu beweisen.
Nachvollziehbarkeit	Die Möglichkeit, Aktivitäten von Subjekten im EVG, die Einfluß auf das Rechenwerk haben, im Nachhinein aufgrund von Aufzeichnungen Schritt für Schritt durchzugehen.
Verbindlichkeit	Die Möglichkeit des Nachweises, daß alle Beteiligten an einer Transaktion ihre Beteiligung an dieser Transaktion nachträglich nicht abstreiten können.
Revisionsdaten	Daten, die zum Nachweis der Ordnungsmäßigkeit und für die Nachvollziehbarkeit gesammelt werden müssen.
Ticket	Eine Sammlung von Daten, die ein Subjekt einem anderen Subjekt vorlegt, um seine Berechtigung zur Durchführung einer Aktion bzw. zur Inanspruchnahme eines Dienstes zu beweisen.

1.4 Bezüge zu anderen Arbeiten

Das vorliegende Schutzprofil basiert auf Arbeiten des Informatikzentrums (SIZ), insbesondere auf der Sicherheitsarchitektur Version 1.0 [SIZSiArch] und dem Sicherheitsstandard Version 2.0 [SIZStd].

1.5 Literaturverzeichnis

[CC] Common Criteria for Information Technology Security Evaluation CCIB-98-026. Version 2.1, August 1999

[SIZSiArch] Erarbeitung einer Sicherheitsarchitektur, SIZ, Version 1.0, November 1996

[SIZStd] SIZ: Standard der IT-Sicherheit. Version 2.0. Oktober 1998

2 Schutzprofil

2.1 Bezeichnung

Der Titel des vorliegenden Schutzprofiles lautet

Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister (SIZ-PP)

Es handelt sich bei diesem Schutzprofil um die Sicherheitsanforderungen der deutschen Sparkassenorganisation an IT-Gesamtsysteme.

2.2 Überblick und Abgrenzung

Das vorliegende Schutzprofil definiert einen Satz grundlegender Sicherheitsanforderungen zur Absicherung von IT-Systemen, wie sie typischerweise im **Kreditgewerbe** bei **Finanzdienstleistern** zum Einsatz kommen. Das Schutzprofil kennzeichnet dabei die **Sicherheitsanforderungen an ein IT-Gesamtsystem**, welches aus Arbeitsplatzrechnern, Servern, Hosts und den sie verbindenden Netzkomponenten und der zum Betrieb der Anwendungen notwendigen Software bestehen kann.

Dieses Schutzprofil ist daher auf Systeme anwendbar, die sich aus Hardwarekomponenten, Betriebssystemen, system- und anwendungsnaher Software (sog. Middleware) sowie Anwendungsprogrammen zusammensetzen.

Die zum Betrieb eines solchen Gesamtsystems erforderliche bauliche, organisatorische und personelle **Infrastruktur** muß bestimmten Sicherheitsanforderungen genügen, die nicht durch den EVG realisiert werden. Daher werden bestimmte Annahmen über die Betriebsumgebung gemacht, ohne die die Sicherheit des IT-Gesamtsystems nicht gewährleistet werden kann. Diese Anahmen finden sich in Abschnitt 4.1.1. wieder.

SIZ-PP-konforme Systeme können in sensitiven Umgebungen des Kreditgewerbes eingesetzt werden, in denen ein hoher Grad an **Vertrauenswürdigkeit** erforderlich ist und in denen die **Vertraulichkeit** und **Integrität** der verarbeiteten Informationen jederzeit gewährleistet sein muß. Die **Verfügbarkeit** der Informationen muß weitestgehend gewährleistet sein, insbesondere sind keine unbemerkten und nicht wiederherstellbaren Verluste von geschäfts- und sicherheitsrelevanten Daten tolerierbar. Für bestimmte Transaktionen wird zudem deren **Verbindlichkeit** sichergestellt.

Systeme, die dem Schutzprofil SIZ-PP genügen, sind in der Lage, Zugriffe auf die von ihnen verwalteten Informationen anhand einer Sicherheitspolitik zu kontrollieren, bei der sowohl

- Zugriffe einzelner Benutzer und Benutzergruppen auf Objekte, die die Informationen enthalten, auf der Grundlage der Ihnen erteilten **Zugriffsrechte**, als auch
- Zugriffe einzelner Benutzer auf anwendungskontrollierte Objekte und Funktionen auf der Basis der von Ihnen ausgeübten **Rollen**

möglich sind.

Das Schutzprofil SIZ-PP bietet einen Schutz, der für eine Umgebung angemessen ist, in der der Zugriff auf Informationen und Systemressourcen auf dazu berechtigte Benutzer beschränkt werden muß. Dabei sind die Benutzer im Rahmen der Ihnen zugeteilten Rechte als vertrauenswürdig anzusehen. Dies gilt insbesondere auch für den Umgang der Benutzer mit den Informationen, deren Dateneigentümer sie sind. Es ist jedoch erforderlich, sie für jede ihrer Aktionen jederzeit zur Verantwortung ziehen zu können.

SIZ-PP fordert daher eine Reihe von Schutzmechanismen, die die Umsetzung der Sicherheitspolitik einer Organisation entsprechend der Vorgaben in Abschnitt 4.3 „Organisatorische Sicherheitspolitik“ sowie die daraus abgeleiteten fachlichen und technischen Sicherheitsanforderungen ermöglichen. Zu diesen Schutzmechanismen gehört neben der oben spezifizierten Zugriffskontrolle die Möglichkeit einer **starken Authentisierung** sowie die Möglichkeit einer **umfassenden Protokollierung und Beweissicherung**.

Von anderen Schutzprofilen unterscheidet sich SIZ-PP dadurch, daß es

- Sicherheitsanforderungen für die Betrachtung von Gesamtsystemen und nicht für einzelne Komponenten formuliert;
- neben einer rollenbasierten Zugriffskontrolle eine benutzerbestimmte Zugriffskontrolle unter der Voraussetzung vertrauenswürdige Dateneigentümer toleriert;
- Anforderungen und Ergebnisse bezüglich der IT-Sicherheit berücksichtigt, die bei der Entwicklung von IT-Systemen im Finanzdienstleistungssektor erarbeitet wurden.

2.3 Stärke der Sicherheitsfunktionen

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil ist

SoF-mittel.

Dies ist die für IT-Systeme im Bereich der Finanzdienstleistungen zu fordernde Sicherheitsstufe, die dessen potentielle Angriffsszenarien abdeckt. Die Stufe „SoF-hoch“ bleibt Systemen vorbehalten, die vor Angreifern mit außerordentlich umfangreichen Ressourcen geschützt werden müssen. Dieses Schutzprofil deckt daher auch keine Anforderungen ab, wie sie sich aus Überlegungen zum „Information Warfare“ für Unternehmen im Finanzdienstleistungssektor ergeben können.

3 Beschreibung des EVG

SIZ-PP beschreibt Sicherheitsanforderungen an IT-Gesamtsysteme für den Einsatz im Kreditgewerbe, die sich aus Hardwarekomponenten, Betriebssystemen, system- und anwendungsnaher Software sowie Anwendungsprogrammen zusammensetzen.

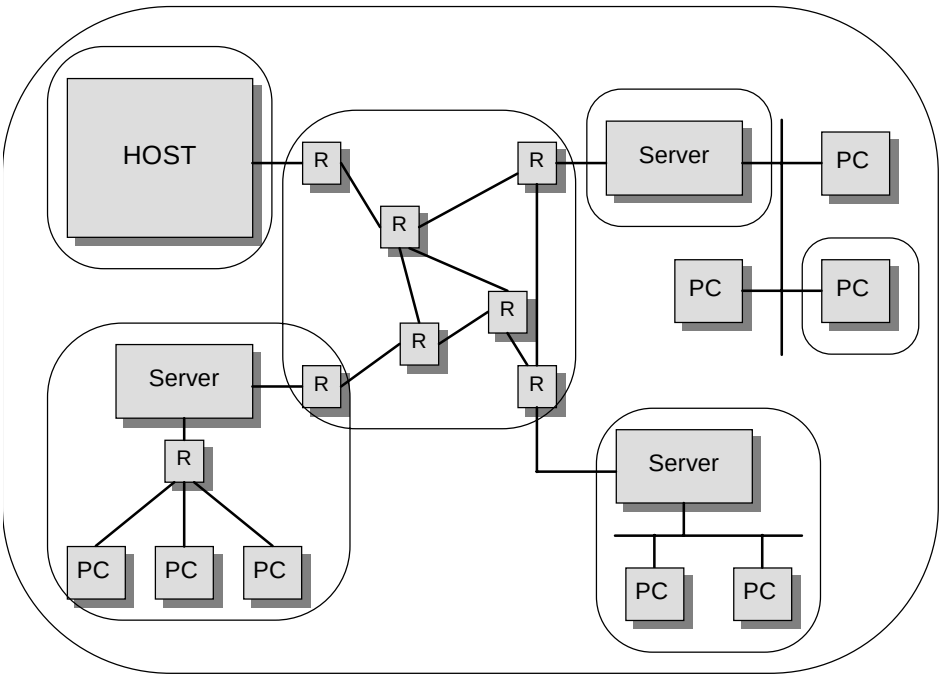

Abbildung 1: Gesamtsystem und mögliche Teilsysteme [2]

Mögliche „Systeme“ werden in Abbildung 1 gezeigt. Die abgerundeten Rechtecke fassen jeweils mehrere Einzelkomponenten zu einem Teilsystem zusammen, welches Gegenstand einer Sicherheitsbetrachtung sein könnte. Jedes dieser Teilsysteme kann in einer Sicherheitsbetrachtung als abgeschlossenes, von den restlichen Teilsystemen unabhängiges System angesehen und bezüglich seiner Sicherheitsfunktionen und seiner Vertrauenswürdigkeit bewertet werden.

Zusammengenommen bilden alle Teilsysteme jedoch ein Gesamtsystem, das die IT-Dienstleistungen für die Organisation erbringt und das in seiner Gesamtheit die Sicherheitspolitik der Organisation umsetzt. Das Gesamtsystem soll die in diesem Schutzprofil beschriebenen Sicherheitsanforderungen umsetzen. Dazu ist jeweils zu spezifizieren, welche Sicherheitsfunktionen in welchen Teilsystemen erbracht werden. Es ist davon auszugehen, daß keines der Teilsysteme in der Lage ist, die in dem vorliegenden Schutzprofil beschriebene Sicherheitsfunktionalität ohne die Mitwirkung anderer Teilsysteme zu erbringen.

[2] R = Router oder Gateway, PC = Arbeitsplatzrechner

4 Sicherheitsumgebung

4.1 Annahmen zum sicheren Betrieb

SIZ-PP-konforme Systeme können die hier beschriebene Sicherheit nur bieten, wenn sie korrekt installiert, verwaltet und benutzt werden. Die Betriebsumgebung muß entsprechend der Dokumentation zur Installation, zur Konfiguration, zum Betrieb und entsprechend der Dokumentation für Benutzer und Systemadministratoren, wie sie im Abschnitt zur Vertrauenswürdigkeit (vgl. Abschnitt 6.2) in diesem Schutzprofil beschrieben sind, administriert werden.

Zusätzlich werden die nachfolgenden Annahmen vorausgesetzt, um die Sicherheit gewährleisten zu können, die dieses Schutzprofil beschreibt.

4.1.1 Annahmen zur Betriebsumgebung

SIZ-PP-konforme IT-Systeme werden in Umgebungen eingesetzt, in denen eine Kontrolle über die physikalischen Einsatzbedingungen der einzelnen Systemkomponenten gegeben ist. Es gelten hierzu folgende Annahmen:

A.Zutritt Einige, jedoch nicht notwendigerweise alle Betriebsmittel des Systems, einschließlich der Arbeitsplätze, befinden sich innerhalb kontrollierter Räumlichkeiten, zu denen nicht befugten Personen der Zugang verwehrt wird.

A.MatSchutz Sämtliche Systemkomponenten, die wesentlich zur Durchsetzung der Sicherheitspolitik sind und die nicht selbst über Vorrichtungen zum Schutz vor unbefugten materiellen Eingriffen und Modifikationen verfügen, sind durch geeignete materielle Maßnahmen vor Eingriffen und Modifikationen durch unbefugte Dritte geschützt.

4.1.2 Annahmen zum Bedienungspersonal

Folgende Annahmen gelten für die personelle Infrastruktur:

A.Admin Es gibt eine oder mehrere ausgebildete Personen, die das System verwalten, einschließlich der Sicherheit der darin verarbeiteten Informationen und der Zuweisung der Betriebsmittel. Diese Personen sind im Rahmen der ihnen übertragenen Aufgaben als vertrauenswürdig zu betrachten.

A.Benutzer Die Benutzer sind für die ihnen übertragenen Aufgaben ausreichend geschult, um die Sicherheitsfunktionen des Systems, soweit sie von ihnen benutzt werden, korrekt und in Übereinstimmung mit der Sicherheitspolitik anzuwenden.

4.1.3 Annahmen zu Kommunikationsverbindungen

Das Schutzprofil **SIZ-PP** geht davon aus, daß die einzelnen verteilten Komponenten des IT-Systems miteinander vernetzt sind. Es werden dabei keine Annahmen über die von den Netzkomponenten selbst zur Verfügung gestellten Sicherheitsmechanismen gemacht. Die für die Sicherung der Übertragung spezifizierten Anforderungen können auf unterschiedlichen Ebenen erbracht werden. Allerdings werden folgende Annahmen für Verbindungen des Systems zu externen Systemen getroffen:

A.Partner Andere Systeme, mit denen ein SIZ-PP-konformes System kommuniziert, unterliegen der gleichen administrativen Kontrolle und werden unter der gleichen Sicherheitspolitik betrieben wie das SIZ-PP konforme System selbst. Damit werden alle verbundenen Systeme zu vertrauenswürdigen Teilsystemen und erfüllen insgesamt das SIZ-PP.

Verbindungen bestehen nur zu Systemen innerhalb einer eigenen Sicherheitsdomäne. Es gibt keine Verbindungen zu Teilsystemen, die eine andere, nicht mit den Zielen der Sparkassenorganisation vereinbare Sicherheitspolitik haben, oder denen nicht vertraut werden kann.

Die Sicherheitsdomäne kann sich dabei über nicht vertrauenswürdige Teilsysteme hinaus erstrecken, falls darüber eine Verbindung zu vertrauenswürdigen Komponenten aufgebaut wird, die durch die nicht vertrauenswürdigen Komponenten nicht manipulierbar ist (z.B. beim Homebanking).

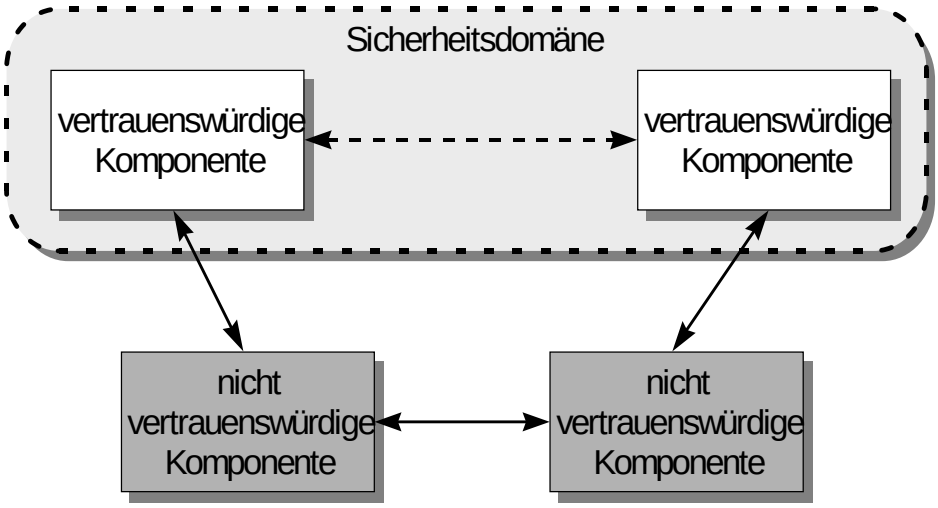

Abbildung 2: Sicherheitsdomäne und nicht vertrauenswürdige Komponenten

Falls die Verbindungen nicht in dem eigenen, kontrollierten Teilsystem liegen, wird sichergestellt, daß die Sicherheitsanforderungen zur Integrität und Vertrauenswürdigkeit der Daten während der Übertragung durch andere Mechanismen, z.B. durch Betreiben eines virtuellen privaten Netzwerkes (VPN) zwischen den Kommunikationsendpunkten, gewährleistet werden.

4.1.4 Annahmen zur organisatorischen Umgebung

Für den Bereich der organisatorischen Umgebung gilt folgende Annahme:

A.SiPol Die organisatorischen und personellen Anteile der in Abschnitt 4.3 „Organisatorische Sicherheitspolitiken“ beschriebenen Sicherheitspolitik sind im Unternehmen mit Unterstützung des Managements umgesetzt

4.2 Bedrohungen

Ein **SIZ-PP**-konformes System muß die in Abschnitt 4.3 „Organisatorische Sicherheitspolitiken“ festgelegte Sicherheitspolitik unterstützen, indem es insbesondere die

- **Verfügbarkeit,**
- **Integrität,**
- **Vertraulichkeit** und
- **Verbindlichkeit** (im Sinne von Authentizität und Nachvollziehbarkeit)

der von ihm verarbeiteten Informationen gewährleistet.

Um die Einhaltung der Sicherheitspolitik zu gewährleisten, müssen die nachfolgend aufgeführten Bedrohungen abgewehrt werden.

4.2.1 Vom EVG abzuwehrende Bedrohungen

Dieser Abschnitt beschreibt die Bedrohungen, die das System aufgrund seiner Sicherheitsfunktionen selbst erkennen und abwehren kann.

B.Zugang **Personen erhalten logischen Zugang zum System, obwohl sie dazu nach der Sicherheitspolitik nicht befugt sind.**

Es muß angenommen werden, daß solche Personen unterschiedlichste Fähigkeiten im Umgang mit dem System besitzen. Personen können eher zufällig aus Neugier oder auch in Kenntnis des Wertes der vom System gespeicherten und verarbeiteten Informationen versuchen, Zugang zum System zu erlangen. Dabei können ihnen Ressourcen in unterschiedlichem Umfang zur Verfügung stehen.

B.Zugriff **Personen erhalten Zugriff auf Informationen in einem Zugriffsmodus, der nach der Sicherheitspolitik nicht erlaubt ist.**

Es muß angenommen werden, daß solche Personen unterschiedlichste Fähigkeiten im Umgang mit dem System besitzen. Obwohl den Benutzern ein gewisses Maß an Vertrauen entgegengebracht wird, die ihnen erteilten Zugriffsrechte nicht zu mißbrauchen, stellt der Wert der im System verarbeiteten und gespeicherten Informationen unter Umständen einen ernstzunehmenden Anreiz für die Benutzer dar, sich in unberechtigter Art und Weise Zugriff auf diese Informationen zu verschaffen.

B.Fehler **Verletzungen der Sicherheitspolitik können durch Fehler in einzelnen Systemkomponenten entstehen.**

Fehler in einzelnen Systemkomponenten können aus dem Nichtvorhandensein von Sicherheitsfunktionen bzw. aus der fehlerhaften Implementierung von Sicherheitsfunktionen resultieren.

Benutzer oder externe Angreifer können solche Fehler, die sie entweder durch zufällige Entdeckung oder durch systematisches Suchen gefunden haben, zur Umgehung der Sicherheitspolitik des Systems und zur Ausübung von Rechten ausnutzen, die ihnen nach der Sicherheitspolitik des Systems nicht zustehen würden.

B.Absturz **Der sichere Betriebszustand des Systems geht bei schweren Ausnahmefehlern verloren.**

Durch Systemabstürze aufgrund schwerwiegender Ausnahmefehler kann die Integrität der Sicherheitsdaten des Systems unbemerkt verlorengehen. Bei Wiederanlauf des Systems ist das System dann unter Umständen nicht mehr in der Lage, die Sicherheitspolitik des Systems korrekt umsetzen.

B.Verfügbarkeit **Berechtigte Benutzer können auf die Informationen und Ressourcen des Systems nicht zugreifen.**

Durch die große Abhängigkeit eines Finanzdienstleistungsunternehmens von seinen Informations- und Kommunikationssystemen ist es für den Geschäftserfolg des Unternehmens unerläßlich, daß Informationen stets dann verwendet und bearbeitet werden können, wenn dies durch die betroffenen Geschäftsprozesse erforderlich ist.

Nichtverfügbarkeit oder eingeschränkte Verfügbarkeit von Informationen und Diensten kann durch verschiedenste Umstände hervorgerufen werden.

B.Beweis **Sicherheitsrelevante Ereignisse werden nicht aufgezeichnet oder können dem Benutzer, der sie ausgelöst hat, nicht eindeutig zugeordnet werden.**

Eine sachgemäße Kontrolle der Sicherheit des Systems kann nur dann erfolgen, wenn sicherheitsrelevante Ereignisse erkannt und aufgezeichnet werden. Es muß stets möglich sein, solche Ereignisse den Benutzern, die sie ausgelöst haben, eindeutig zuzuordnen. Auch die Aufzeichnung dieser sicherheitsrelevanten Ereignisse muß vor Manipulation, Zerstörung und unerlaubtem Zugriff geschützt werden.

Wenn diese Voraussetzungen nicht erfüllt sind, kann eine angemessene Reaktion auf Attacken gegen das System nicht mehr gewährleistet werden.

B.Manipulation **Manipulation sicherheitsrelevanter Mechanismen ist möglich.**

Die Systemmodule und Daten, die für die Durchsetzung der Sicherheitspolitik des Systems verantwortlich sind, können umgangen oder manipuliert werden. Dadurch kann die Integrität der Sicherheitsmechanismen verletzt und die Durchsetzung der Sicherheitspolitik des Systems nicht mehr gewährleistet sein.

B.Erkennen **Ereignisse während des Betriebes, die die Sicherheit des Systems verletzen, werden nicht rechtzeitig erkannt.**

Diese Bedrohung besteht aufgrund der menschlichen Schwäche der Systemadministratoren, auftretende Probleme im Zusammenhang mit der Systemsicherheit nicht zuverlässig erkennen zu können. Dies kann dazu führen, daß beim Nichterkennen von aufgetretenen Sicherheitsproblemen das System in einem unsicheren Zustand weiter betrieben wird und die Systemadministratoren weiterhin davon ausgehen, daß sich das System in einem sicheren Zustand befindet.

Ausgelöst werden kann das Nichterkennen von Sicherheitsproblemen z.B. durch das Nichterkennen von Meldungen, oder durch fehlende, unverständliche oder unvollständige Meldungen.

4.2.2 Von der Betriebsumgebung abzuwehrende Bedrohungen

Die nachfolgend aufgeführten Bedrohungen müssen abgewehrt werden, um die Sicherheit eines SIZ-PP-konformen Systems zu gewährleisten. Da das System sie jedoch nicht selbst abwehren kann, muß in der Betriebsumgebung Vorsorge für ihre Abwehr getroffen werden. Die Abwehr dieser Bedrohungen ist nicht Bestandteil der Sicherheitsfunktionalität, die ein SIZ-PP-konformes System erbringt.

B.Installation **Das System kann in einem unsicheren Zustand ausgeliefert und installiert werden.**

Wurde ein SIZ-PP-konformes System in einem unsicheren Zustand geliefert oder installiert, können sicherheitsrelevante Funktionalitäten des Systems unter Umständen nicht aktiv sein oder durch Benutzer umgangen bzw. ausgeschaltet werden. Der sichere Betrieb des SIZ-PP-konformen Systems kann dann nicht mehr gewährleistet werden.

B.Betrieb **Durch Fehler in Administration und Betrieb des Systems kommt es zu Verletzungen der Sicherheitspolitik.**

Die Sicherheit eines SIZ-PP-konformen Systems kann nur dann gewährleistet werden, wenn Systemadministratoren und Benutzer, die sicherheitsrelevante Funktionen ausführen dürfen, das System korrekt benutzen.

Solche Bedrohungen können durch Fehler in der Administration des Systems ausgelöst werden, z.B. durch das versehentliche Ausschalten von Sicherheitsmechanismen oder durch fehlerhafte Wiederanlaufprozeduren, die einen unsicheren Systemzustand herbeiführen.

Benutzer oder externe Angreifer können Unzulänglichkeiten in der Administration und im Betrieb des Systems, die sie durch zufällige Entdeckung oder durch systematisches Suchen gefunden haben, ausnutzen, um die Sicherheitspolitik des Systems zu umgehen und Rechte auszuüben, die ihnen nach der Sicherheitspolitik des Systems nicht zustehen würden.

B.Rollen **Die Definition und die Zuweisung von Rollen geschieht so, daß die Sicherheitspolitik verletzt wird.**

Durch die Definition einer Vielzahl unterschiedlicher Rollen im Rahmen eines Rollenkonzeptes können Rechtekombinationen für einzelne Benutzer entstehen, die im Widerspruch zur Sicherheitspolitik des Unternehmens stehen. Jede einzelne Rolle kann dabei für sich allein die Anforderungen der Sicherheitspolitik erfüllen, jedoch können durch Zuweisung mehrerer Rollen an einen Benutzer kombinierte Rechte dieses Benutzers entstehen, die über die Rechte der einzelnen Rollen hinausgehen und damit die Sicherheitspolitik bei Ausübung dieser Rechtekombinationen verletzen.

Ebenso können Benutzer solche Rollen zugewiesen bekommen, die sie aufgrund ihrer tatsächlichen Pflichten nicht einnehmen dürften. Dadurch können Benutzer Zugriff auf Bereiche des Systems erhalten, für die sie aufgrund ihrer Funktion im Unternehmen nicht berechtigt sind.

Ein besonderes Problem stellt die Möglichkeit einer Zuweisung von sich gegenseitig ausschließenden Rollen an einen Benutzer dar.

B.Gewalt **Durch äußere Gewalteinwirkung können sicherheitskritische Komponenten des Systems manipuliert oder außer Funktion gesetzt werden.**

Werden Komponenten des SIZ-PP-konformen Systems durch äußere Gewalteinwirkung ausgeschaltet oder in ihrer Funktion beeinträchtigt, können die darauf aufbauenden, im wesentlichen auf logischen Kontrollen basierenden Sicherheitsfunktionen des Systems ihre Leistungen nicht mehr oder nur in vermindertem Umfang erbringen. Nach einer erfolgreichen Manipulation der sicherheitskritischen Komponenten kann ein sicherer Betrieb des SIZ-PP-konformen Systems nicht mehr sichergestellt werden.

4.3 Organisatorische Sicherheitspolitiken

Das Geschäftsziel eines Unternehmens im Kreditgewerbe ist die Abwicklung aller Bankgeschäfte zur Zufriedenheit des Kunden bzw. der Geschäftspartner sowie der Aufbau von Vermögenswerten. Jede Sicherheitspolitik für ein Finanzdienstleistungsunternehmen muß sich an diesem obersten Geschäftsziel ausrichten.

SIZ-PP-konforme Systeme sind in der Lage, eine breite Klasse von Sicherheitspolitiken einer Organisation zu unterstützen. Insbesondere sind sie in der Lage, Sicherheitspolitiken von Unternehmen im Kreditgewerbe, wie sie durch die Geschäftsziele, die Geschäftsprozesse und ihre Einbettung in ein rechtliches Rahmenwerk vorgegeben werden, effizient umzusetzen.

Die nachfolgend wiedergegebene Sicherheitspolitik der Sparkassenorganisation (vgl. [SIZSiArch]) umfaßt Sicherheitsgrundsätze und -strategien, die nicht allein durch technisch-organisatorische IT-Sicherheitsmaßnahmen umgesetzt werden können. Die Umsetzung dieser Politik erfordert organisatorische und personelle Maßnahmen, die nicht Bestandteil der Anforderungen dieses Schutzprofiles sind. Ihre Umsetzung wird dennoch vorausgesetzt, um die hier beschriebene Sicherheit des IT-Gesamtsystems zu gewährleisten (vgl. Annahme A.SiPol).

4.3.1 Grundsätze der IT-Sicherheitspolitik (Sicherheitsgrundsätze)

Innerhalb der Sparkassenorganisation gelten die folgenden Sicherheitsgrundsätze, die in dieser Form auch auf andere Unternehmen des Kreditgewerbes anwendbar sind:[3]

G1 **Sicherheitspolitik als integraler Bestandteil der Geschäftspolitik**

Die Festschreibung des Sicherheitsaspektes ist integraler Bestandteil der Geschäftspolitik der Sparkassenorganisation.

G2 **Einhaltung der gesetzlichen Anforderungen**

Die Einhaltung aller bundesdeutschen, landesweiten und europäischen Gesetze und Berücksichtigung der ergänzenden Regelungen bezüglich der IT-Sicherheit ist verbindlich.

G3 **Schutz von Daten und Ressourcen**

Das Unternehmen gewährleistet die Integrität, die Verbindlichkeit, die Vertraulichkeit und die Verfügbarkeit ihrer eigenen und der ihr anvertrauten Daten und Ressourcen. Dies gilt sowohl auf den eigenen Systemen als auch auf den Systemen, die der Verantwortung des Unternehmens unterstehen.

G4 **Sicherheit als Schutz der Mitarbeiter, Partner und Kunden**

Im Rahmen der eingesetzten Anwendungssysteme werden alle Sicherheitsdienstleistungen sowie Soft- und Hardware bereitgestellt, um alle an der Informationsverarbeitung beteiligten Mitarbeiter, Partner und Kunden von mißbräuchlicher Benutzung von Daten und Ressourcen abzuhalten und vor ungerechtfertigter Verdächtigung zu schützen.

---

[3] Die Zählung der Grundsätze und Sicherheitsstrategien entspricht der Zählweise aus [SIZSiArch].

G5 **Gewährleistung der Nachvollziehbarkeit**

Die Nachvollziehbarkeit aller relevanten Aktivitäten im System ist eine unabdingbare Forderung, sowohl aus entsprechenden gesetzlichen bzw. geschäftlichen Anforderungen als auch aus Eigeninteresse des jeweiligen Unternehmens. Ziel muß es sein, auch im Umfeld verteilter Anwendungen den für eine Aktion Verantwortlichen eindeutig feststellen zu können. Ebenso muß Beweismaterial für Streitfälle erstellt und aufbewahrt werden.

G6 **Einhaltung von Standards und Regelwerken**

Alle sicherheitsrelevanten Aktivitäten werden in Standards und Regelwerken niedergelegt, die ständig an alle sich ändernden Anforderungen angepaßt und gegebenenfalls erweitert werden müssen [4].

4.3.2 Sicherheitsstrategien / Sicherheitspolitiken

Die im vorigen Abschnitt benannten Sicherheitsgrundsätze werden durch die nachfolgenden Sicherheitsstrategien umgesetzt, die ebenfalls integraler Bestandteil der Sicherheitspolitik in einer SIZ-PP-konformen Systemumgebung sind.

4.3.2.1 Sicherheitsstrategien zu G1

S1.1 **Umsetzung und Einhaltung der Maßnahmen als Managementaufgabe**

Um IT-Sicherheit in allen Ebenen des Unternehmens wirksam umsetzen zu können, ist es die Aufgabe des Managements, notwendige Rahmenbedingungen zur Verfügung zu stellen. Die Grundsätze der IT-Sicherheitspolitik müssen in die jeweils erforderlichen Sicherheitsinstrumente der Institution einfließen und umgesetzt werden. Die Einhaltung der Sicherheitsgrundsätze ist sicherzustellen.

Das Management muß dabei eine Vorbildfunktion ausüben. Wichtig ist eine Vermittlung der Schutzfunktion, die jedem Mitarbeiter durch die Einhaltung der Verfahren zu Gute kommt. Sicherheit darf von den Mitarbeitern nicht als hinderlich angesehen werden.

S1.2 **Etablierung eines Verfahrens „Sicherheitsmanagement“ im Prozeßmodell des Unternehmens**

Im Prozeßmodell des Unternehmens wird ein Prozeß „IT-Sicherheitsmanagement” eingeführt.

Durch den Prozeß „IT-Sicherheitsmanagement” wird die Gesamtthematik IT-Sicherheit in den Prozessen des Unternehmens verankert.

Es erfolgt eine Festlegung eines Verantwortlichen (Rolle IT-Sicherheitsmanager) für IT-Sicherheitsbelange durch die Geschäftsführung. Der Zuständigkeitsbereich dieses Verantwortlichen umfaßt den Aufbau, die Durchführung und die Überwachung der IT-Sicherheits-Organisation des Unternehmens.

In das IT-Sicherheitsmanagement fließen Ergebnisse aus dem gesetzlichen Umfeld des Sicherheitsgrundsatzes G2 ein.

---

[4] Dieses Schutzprofil selbst resultiert direkt aus der Umsetzung dieses Grundsatzes.

S1.3 Durchgängige Gewährleistung von IT-Sicherheit in neuen Anwendungssystemen / Releases

Der Stellenwert der IT-Sicherheit wird für alle Produkte als strategisch wichtig erklärt. Dies ist besonders für neue Anwendungssysteme / Releases von Bedeutung und betrifft sowohl den Vorgang der Anwendungsentwicklung selbst als auch die notwendige Infrastruktur innerhalb der Anwendungsentwicklung.

Die IT-Sicherheit wird von der Produktdefinition bis zur Produkteinführung durchgängig gewährleistet. Der Kunde/Anwender ist aktiv an der Formulierung von Sicherheitsanforderungen der Produkte beteiligt und wird in der Anwendung der Sicherheitsfunktionen der Produkte geschult. Der Kunde wird auf Gefahren der Kompromittierung der Systeme hingewiesen.

Das IT-Sicherheitsmanagement formuliert die Sicherheitsanforderungen für die betroffenen Bereiche und Prozesse, berät diese bei der Auswahl von Verfahren und Methoden und unterstützt diese bei der Umsetzung in Sicherheitsbelangen.

S1.4 Erklärung eines verbindlichen Anwendungsentwicklungsmodells für die Anwendungsentwicklung

Das Anwendungsentwicklungsmodell muß Methoden und Verfahren für die Integration von Sicherheitsanforderungen von der Produktdefinition über sämtliche Stufen des Lebenszyklus der Anwendung hinweg definieren.

Dies betrifft sowohl Methoden und Verfahren für die inhaltliche Sicherheit der entwickelten Anwendungen und Releases als auch die Gestaltung des Anwendungsentwicklungsprozesses in einer sicheren Art und Weise, unter Berücksichtigung von IT-Sicherheitsanforderungen.

S1.5 Durchsetzung der IT-Sicherheit in Betrieb und Produktion

Der hohe Stellenwert der IT-Sicherheit wird in allen Bereichen durch die Einhaltung und Umsetzung der IT-Sicherheitspolitik zum Ausdruck gebracht und gewährleistet. Es wird eine Infrastruktur eingesetzt und genutzt, die die Umsetzung der Sicherheitspolitik und der Sicherheitsanforderungen unterstützt.

Dies gilt sowohl für eigene eingesetzte DV-Systeme des Rechenzentrumsbetriebs, für die Anwendungsentwicklung als auch für DV-Systeme der Büroautomation im Betrieb, unabhängig ob im zentralen oder dezentralen Bereich, auf hostbasierten oder dezentralen Systemen.

Die DV-Systeme werden entsprechend den Sicherheitsanforderungen der Sicherheitspolitik eingeführt, eingesetzt oder erweitert.

Die internen und externen Sicherheitssysteme sind entsprechend den Sicherheitsanforderungen des Unternehmens, des Kunden und der Partner zur Verfügung zu stellen, zu nutzen und zu verwalten.

Die korrekte Benutzung der Systeme wird dokumentiert, die sicherheitsgemäße Benutzung der Systeme geschult und regelmäßig trainiert.

Regelmäßige Sicherheitskontrollen halten das Verhalten des Systems und seiner Benutzer fest und bewerten dieses durch entsprechende Analysen. Bei Erkennen von Risiken werden entsprechende Maßnahmen eingeleitet.

Die Verfügbarkeit der Daten und Anwendungssysteme wird durch verläßliche Konzepte für Datensicherung und Wiederanlauf gewährleistet. Archivierungskonzepte und -systeme setzen die gesetzlichen oder institutseigenen Anforderungen um. Notfallkonzepte beschreiben notwendige Verfahren und bereiten die sichere Reaktion auf Ausnahmesituationen vor.

S1.6 Organisationsinterne Verdeutlichung und verbindliche Erklärung des hohen Stellenwertes der IT-Sicherheit

Der hohe Stellenwert, den die IT-Sicherheit im Unternehmen innehat, wird im Unternehmen verdeutlicht und als verbindlich erklärt.

Innerhalb der Führungsebenen muß IT-Sicherheit als Managementaufgabe verstanden werden. Innerhalb der fachlichen Ebene muß das Sicherheitsbewußtsein der Mitarbeiter durch geeignete Maßnahmen gefördert werden. Notwendige IT-Sicherheitsmaßnahmen dürfen von den Mitarbeitern nicht als hinderlich empfunden und betrachtet werden.

S1.7 Förderung des Sicherheitsbewußtseins

Die Benutzer (Mitarbeiter, Kunden und Partner) sind regelmäßig über die konkreten Auswirkungen zu informieren und zu schulen, die sich durch die Anforderungen im gesetzlichen Umfeld und ergänzenden Richtlinien für die IT-Sicherheit ergeben. Alle Beteiligten sollen über die sich ergebenden Konsequenzen und die daraus resultierenden Rechte und Pflichten informiert sein, die für seinen Verantwortungsbereich gültig sind.

Die Erläuterung notwendiger Sicherheitsrichtlinien werden das Verständnis und die Akzeptanz aller Beteiligten fördern.

Veröffentlichungen und Schulungen werden um entsprechende Informationen ergänzt, die sich aus den Erfordernissen des gesetzlichen Umfeldes und ergänzenden Richtlinien ergeben.

Zur Förderung des Sicherheitsbewußtseins werden Beiträge für Personalzeitschriften, Anzeigen und andere betriebsinterne Kommunikationsmittel zur Verdeutlichung der Sicherheitsgrundsätze und ihrer Bedeutung für das Unternehmen entwickelt. Dabei sollen nach Möglichkeit Beispiele für mangelnde Sicherheit und deren negative geschäftliche Konsequenzen oder für die Schadensvermeidung durch die Anwendung angemessener Sicherheitsstandards angeführt werden.

S1.8 Betonung des Schutzcharakters von Sicherheit

Es werden Informationsmaterial und -programme (für interne Zeitschriften, Anzeigen, Videos, etc.) entworfen, die der Unterrichtung der Mitarbeiter über die definierte Sicherheitspolitik und zur Darstellung der Probleme dienen, die durch unzureichende Sicherheit entstehen können. Diese Materialien sind auch für Partner und Kunden zu entwickeln.

Notwendige IT-Sicherheitsmaßnahmen dürfen nicht als „lästiges Übel“ verstanden werden. Diese Maßnahmen schützen ebenfalls das von Mitarbeitern, Partnern und Kunden Geleistete.

S1.9 Verdeutlichung und Betonung des hohen Stellenwertes der IT-Sicherheit gegenüber Kunden und Partnern

Gegenüber Kooperationspartnern, Mitentwicklern, Kunden des Unternehmens und möglichen anderen Partnern wird die strategische Ausrichtung der IT-Sicherheit verdeutlicht. Ein hohes Sicherheitsniveau stellt ein unver-

zichtbares Qualitätsmerkmal eines Produktes und des Services dar und ist ein Charakteristikum im Bereich der Nutzung und der Bereitstellung der Anwendungssysteme. Erfolgreich umgesetzte IT-Sicherheitsmaßnahmen können ein Wettbewerbsfaktor sein.

Kunden und Partnern werden die Risiken verdeutlicht, die durch Nichtbeachtung der Sicherheitsanforderungen entstehen und zu einer Kompromittierung sensibler Systemanteile führen können.

4.3.2.2 Sicherheitsstrategien zu G2

S2.1 Herstellung der Gesetzeskonformität

Die geltenden gesetzlichen Anforderungen für das Unternehmen müssen untersucht, der Ist-Status festgehalten und dokumentiert werden.

Durch regelmäßige Beobachtung der Gesetzgebung und relevanter Richtlinien muß der Status aktualisiert werden.

S2.2 Einflußnahme auf Gesetze und Regelungen

Eine Mitwirkung an Standardisierungsorganisationen und -gremien ist vorzusehen, um sicherzustellen, daß die Interessen der Sparkassenorganisation und des Unternehmens gewahrt bleiben.

Wo möglich, sollte sich das Unternehmen an der Formulierung von Standards im Sicherheitsbereich beteiligen und sich damit die Möglichkeit verschaffen, seine Interessen in geeigneten Gremien zu vertreten.

4.3.2.3 Sicherheitsstrategien zu G3

S3.1 Festlegung von Verantwortungsbereichen innerhalb der beteiligten Systeme und Netze

Das Unternehmen legt zusammen mit allen Beteiligten IT-Verantwortungsbereiche innerhalb der beteiligten Systeme und Netze fest. Die Verantwortlichen müssen mit entsprechenden Kompetenzen ausgestattet sein, um ihre Verantwortung ausführen zu können.

Erforderliche Schnittstellen zwischen unterschiedlichen Verantwortungsbereichen müssen definiert werden.

S3.2 Gewährleistung der Integrität von Daten, Programmen und Ressourcen

Das Unternehmen stellt durch technische und organisatorische Maßnahmen sicher, daß die Integrität von Daten, Programmen und Ressourcen, für die das Unternehmen die Verantwortung trägt, gewährleistet ist.

Durch diese Maßnahmen wird gewährleistet, daß Daten und Programme nur von dem dazu berechtigten Personenkreis erzeugt, modifiziert und gelöscht werden können. Dies setzt eine korrekte Zuordnung von Daten zu Benutzern oder Prozessen voraus.

Veränderungen an Daten und Programmen sowie deren Verlust müssen zuverlässig erkannt werden können.

S3.3 Gewährleistung der Verbindlichkeit von Daten und Programmen

Das Unternehmen stellt durch technische und organisatorische Maßnahmen sicher, daß die Verbindlichkeit von Daten und Programmen, für die das Unternehmen die Verantwortung trägt, gewährleistet ist.

S3.4 Gewährleistung der Vertraulichkeit von Daten und Programmen

Das Unternehmen stellt durch geeignete technische und organisatorische Maßnahmen sicher, daß die Vertraulichkeit von Daten und Programmen, für die das Unternehmen die Verantwortung trägt, gewährleistet ist.

Die gesetzlichen Anforderungen des Datenschutzgesetzes werden für alle personenbezogene Daten eingehalten, die das Unternehmen verarbeitet.

Daten und Programmen des Unternehmens und ihm von seinen Kunden anvertraute Daten unterliegen der Geheimhaltung. Gleiches gilt für Informationen über die Existenz solcher Daten und Programme. Jede zwischen den Organisationen und den Kunden weitergegebene Information wird entsprechend den spezifischen Anforderungen genauso vertraulich behandelt wie die Tatsache der Informationsweitergabe selbst.

S3.5 Gewährleistung der Verfügbarkeit von Daten und Programmen

Das Unternehmen stellt die Verfügbarkeit aller Daten und Programme sicher, für die es die Verantwortung trägt. Dies geschieht durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen.

S3.6 Funktionstrennung

Aufgaben, die von unterschiedlichen Personen oder Prozessen durchgeführt werden sollen, werden durch geeignete technische oder organisatorische Maßnahmen voneinander getrennt. Für alle sensitiven Aufgaben wird im Unternehmen das Vier-Augen-Prinzip unter Berücksichtigung der dazu erforderlichen, zusätzlichen Authentisierungsverfahren durchgesetzt.

S3.7 Rollen- und Aufgabenidentifizierung

Die Aufgabe und die Rolle, die von einem berechtigten Benutzer zu einem bestimmten Zeitpunkt ausgeübt wird, sind aufgrund der eindeutigen Zuordnung jederzeit klar erkennbar und nachvollziehbar.

S3.8 Zugriffskontrolle zu Ressourcen

Eine Zugriffskontrolle ermöglicht die Überprüfung von Rechten und im Anschluß daran die Zulassung bzw. Rückweisung von Aktionen. Die Zugriffskontrolle ist bei allen Aktivitäten auf Programmen, Dateien, Transaktionen, Befehlen, Jobs oder anderen Einheiten und Objekten entsprechend deren jeweiligen Schutzanforderungen erforderlich. Die Zugriffskontrolle bei Ressourcen wird auf Grundlage der Funktionen bzw. Rollen durchgeführt.

S3.9 Identifikation aller Kommunikationspartner[5]

Alle Kommunikationspartner, die IT-Dienstleistungen innerhalb des Unternehmens oder für das Unternehmen erbringen, sollen jederzeit eindeutig identifiziert werden können, unabhängig vom Beschäftigungsstatus oder der Beziehung zum Unternehmen.

---

[5] Diese Sicherheitsstrategie umfaßt vollständig die Sicherheitsstrategien S3.10 „Authentisierungsdienst“, S3.11 „Systemauthentisierung“, S3.12 „Benutzeridentifikation“ und S3.13 „Gegenseitige Ende-zu-Ende-Authentisierung“ aus [SIZSiArch], die daher hier nicht noch einmal aufgeführt werden. Um die Querverbindungen zu [SIZSiArch] zu vereinfachen, wurde die Zählung der Sicherheitsstrategien beibehalten, weshalb zwischen S3.9 und S3.14 eine Lücke entsteht.

S3.14 Archivierung und Nachvollziehbarkeit

Mit Hilfe von Archivierungseinrichtungen bestehen Möglichkeiten, Programme inklusive Dokumentation und die dazugehörigen Datenbestände einschließlich der erforderlichen Protokollinformationen entsprechend den gesetzlichen und geschäftlichen Anforderungen aufzubewahren, um so jederzeit eine Wiederherstellung einer bestimmten Verarbeitungsumgebung und der erforderlichen Dokumentation zu gewährleisten.

4.3.2.4 Sicherheitsstrategien zu G4

S4.1 Vermeidung von Interessenskonflikten für Mitarbeiter durch geeignete organisatorische und technische Maßnahmen

Der Schutz des Mitarbeiters ist grundsätzlich bei allen Maßnahmen zur IT-Sicherheit zu berücksichtigen. Dabei muß vorausgesetzt werden, daß die Identität des Mitarbeiters eindeutig feststellbar ist, da sonst Handlungen, die der Mitarbeiter für das Unternehmen ausführt, dem Mitarbeiter nicht zugeordnet werden können und diesem daher keine Verantwortung für seine Aktivitäten übertragen werden kann. Zugriffsrechte werden basierend auf den jeweiligen Rollen vergeben, die ein Mitarbeiter zum Zeitpunkt der Vergabe der Zugriffsrechte ausübt.

Zur Vermeidung von Interessenskonflikten müssen Rollen so festgelegt werden, daß eine klare Funktionstrennung möglich ist.

S4.2 Nutzung von Systemen nur nach erfolgreicher Identifikation und Authentisierung

Die Nutzung von Systemen und Ressourcen darf nur nach erfolgreicher Identifikation und Authentisierung erfolgen, es sei denn, für den genutzten Dienst ist weder eine Zugriffskontrolle noch eine Beweispflicht gefordert.

Identifikation und Authentisierung gewährleisten eine eindeutige Bestimmbarkeit von Benutzern und Systemen. Diese ist für weitere Sicherheitsdienste wie z.B. Kontrolle des Zugriffs auf Ressourcen oder Nachweisbarkeit von Handlungen unabdingbar.

Bei Kommunikationsbeziehungen muß gewährleistet sein, daß identifizierte Benutzer bzw. Rollen und deren Authentisierungsstatus gesichert weitergereicht werden.

S4.3 Klare Beschreibung der Sicherheitspolitik

Die Sicherheitspolitik und die daraus resultierenden Konsequenzen müssen klar beschrieben werden, so daß sie von allen mit der Informationsverarbeitung befaßten Mitarbeitern verstanden werden können.

Falls eine Umgehung von Sicherheitsmaßnahmen erforderlich sein sollte, muß es Verfahren zur formalen Absicherung der Mitarbeiter geben, so daß Mitarbeiter für Probleme, die aus einer solchen Umgehung resultieren können, nicht verantwortlich gemacht werden können.

S4.4 Mitarbeitereinsatz

Der Einsatz von Mitarbeitern und die Festlegung ihrer Rollen und Funktionen ist jederzeit durch eine nachvollziehbare Dokumentation belegbar. Insbesondere werden alle Aktivitäten in Bezug auf Vereinbarung, Aufgabenstellung, Durchführung sowie angegliederte Funktionen der Sicherheitsad-

ministration in der jeweiligen Institution aufgezeichnet und regelmäßig kontrolliert.

Die Pflichten aller Mitarbeiter im IT-Sicherheitsbereich sind durch klare und präzise Definition der Erfordernisse und Verantwortung zu spezifizieren. Jeder Mitarbeiter, der in die Verwaltung des Sicherheitssystems involviert ist, muß seine Verantwortung klar verstehen und als verbindlich akzeptieren. Diese Erklärungen werden die Aspekte der Vertraulichkeit der verwendeten Daten und die Anerkennung rechtlicher Verantwortung beinhalten.

S4.5 Festlegung von Absicherungsverfahren

Sollte es in ungewöhnlichen Situationen notwendig sein, die bestehenden Sicherheitsmaßnahmen zu umgehen, muß dies dokumentiert werden.

Es muß klar geregelt sein, wie die Umgehung der Sicherheitsmaßnahmen zu geschehen hat, welche Maßnahmen vor, während und nach der Umgehung zu treffen sind, und wer die Verantwortung für die Umgehung und alle daraus resultierenden Folgen trägt.

S4.6 Risikobewertung einzelner Aufgaben und Funktionen

Risikoanalysen dienen der Verbesserung der Kommunikation zwischen technischem bzw. fachlichem Management und Vorstand, indem ein komplettes Bild der Sicherheitsumgebung und deren Einfluß auf Geschäftsaktivitäten präsentiert wird.

4.3.2.5 Sicherheitsstrategien zu G5

S5.1 Umsetzung der Anforderungen an Nachvollziehbarkeit, Beweispflicht und Revisionsfähigkeit, die sich aus Gesetzen, Regelungen und Anforderungen der Sparkassenorganisation ergeben

Die Anforderungen in den Bereichen Nachvollziehbarkeit, Beweispflicht und Revisionsfähigkeit resultieren aus den gesetzlichen Regelungen und ergänzenden Richtlinien und aus den Erfordernissen der Sparkassenorganisation und den ihr angeschlossenen Unternehmen. Dies betrifft sowohl die Datenbasis als auch Fristen und Form der Aufbewahrung von Informationen.

S5.2 Festlegung organisationseigener Sicherheitsanforderungen bezüglich Nachvollziehbarkeit, Beweispflicht und Revisionsfähigkeit

Aus Gründen der Schadensabwehr kann es im Eigeninteresse des Unternehmens erforderlich sein, eigene Anforderungen festzulegen, die über die bestehenden gesetzlichen Regelungen hinausgehen.

S5.3 Ermittlung und Erzeugung von Daten zur Nachvollziehbarkeit

Es werden Dienste eingesetzt, die die erforderlichen Daten zur Nachvollziehbarkeit einschließlich der Daten zur Beweispflicht und Revisionssicherheit fälschungssicher erzeugen. Die aufzuzeichnenden Informationen sind i.a. anwendungsbezogen festgelegt. Alle Informationen, die zum personen- bzw. rollenbezogenen Nachweis notwendig sind, werden von Anwendungssystemen zur Verfügung gestellt.

S5.4 **Bereitstellung und Schutz von Revisionsdaten**

Die Anwendungssysteme des Unternehmens stellen jederzeit alle revisionsrelevanten Daten zur Verfügung.

Die revisionsrelevanten Daten werden durch geeignete technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

S5.5 **Sichere Aufbewahrung der beweisrelevanten Informationen**

Alle notwendigen Kontrollinformationen werden gemäß den gesetzlichen, handelsrechtlichen Erfordernissen sowie den Standards und Regelungen der Sparkassenorganisation aufbewahrt.

S5.6 **Unleugbarkeit aller geschäftlichen Transaktionen**

Anwendungsprogramme und -systeme werden so entwickelt, daß Transaktionen, die unter ihrer Kontrolle stehen, weder vom Initiator bzw. Sender noch vom Ausführenden bzw. Empfänger geleugnet werden können.

Prüfverfahren beinhalten diesen Beweis der Unleugbarkeit.

4.3.2.6 Sicherheitsstrategien zu G6

S6.1 **Beschreibung der Sicherheitspolitik mit allen zugehörigen Aspekten**

Sicherheitspolitik und IT- Sicherheitsstandard werden so formuliert, daß sie dem aktuellen Stand der Technik entsprechen und alle rechtlichen und ergänzenden Anforderungen, insbesondere aus dem Bereich der Sparkassenorganisation, abdecken, die zur Gewährleistung des Schutzes von Benutzern, Daten und Ressourcen notwendig sind.

Der IT-Sicherheitsstandard (und davon abgeleitet dieses Schutzprofil) bildet einen Katalog von Mindestanforderungen, die von allen derzeitigen und zukünftigen Systemen bzw. Teilsystemen zu erfüllen sind, um die Sicherheit der Anwendungen zu gewährleisten.

Die Einhaltung der Sicherheitspolitik und des IT-Sicherheitsstandards sind eine Voraussetzung für Neuentwicklungen.

S6.2 **Regelmäßiger Nachweis und Dokumentation der Einhaltung von Standards und Regelwerken**

Alle im Sicherheitsstandard beschriebenen Kontrollverfahren werden im Unternehmen regelmäßig durchgeführt. Die Ergebnisse der Kontrollen werden revisionsfähig dokumentiert.

S6.3 **Fortschreibung und Anpassung der Standards und Regelwerke**

Alle relevanten Sicherheitsstandards und Regelwerke werden in regelmäßigen Intervallen überprüft und an den Stand der Technik und an neue Sicherheitsanforderungen angepaßt.

5 Sicherheitsziele

Zur Abwehr der in Abschnitt 4.2 „Bedrohungen“ spezifizierten Bedrohungen und zur Umsetzung der technisch-organisatorischen Anteile der oben dargelegten Sicherheitspolitik ergeben sich die nachfolgenden Sicherheitsziele, die von einem SIZ-PP-konformen System und seiner Betriebsumgebung erfüllt werden müssen.

Die Zusammenhänge zwischen Sicherheitspolitik und Sicherheitszielen werden im Anhang in Abschnitt 8.2.2 erläutert, die Zusammenhänge zwischen Bedrohungen und Sicherheitszielen in Abschnitt 8.2.1.

5.1 Sicherheitsziele für den EVG

Nachfolgend werden die Sicherheitsziele des EVG aufgeführt, die für die Abwehr der identifizierten Bedrohungen und die Umsetzung der Sicherheitspolitik des EVG erforderlich sind.

Z.Zugang Das System unterbindet jeglichen logischen Zugang von unbefugten, d.h. nicht berechtigten Personen bzw. Kommunikationspartnern zum System. Dies kann beispielsweise bedeuten, dass sich jeder Benutzer identifizieren und authentisieren muß, bevor der logische Zugang zum System gewährt wird.

Z.Zugriff Das System verhindert, daß Benutzer Zugriff zu Informationen oder Ressourcen des Systems erhält, für die er aufgrund seiner Rolle oder seiner individuellen Berechtigung keine Zugriffsrechte besitzt.

Z.Archiv Das System ermöglicht, Programme inklusive Dokumentation und die dazugehörigen Datenbestände entsprechend den gesetzlichen und geschäftlichen Anforderungen zu archivieren, um so eine Wiederherstellung einer bestimmten Verarbeitungsumgebung und der erforderlichen Dokumentation zu gewährleisten.

Z.Verantwortung Das System stellt sicher, daß alle Benutzer für ihre sicherheitsrelevanten Aktionen zur Verantwortung gezogen werden können. Dies bedeutet, daß das System in der Lage ist,

- alle zur Nachvollziehbarkeit, Beweispflicht und Revisionssicherheit notwendigen Daten fälschungssicher zu erzeugen. Die aufzuzeichnenden Informationen sind anwendungsbezogen festzulegen. Alle zum personen- bzw. rollenbezogenen Nachweis benötigten Informationen sind von Anwendungssystemen zur Verfügung zu stellen.
- alle vom System erfaßten revisionsrelevanten Daten werden im System gesichert abgelegt. Der Zugriff auf diese Daten ist nur besonders priviligierten Personen, z.B. Administratoren oder Auditoren möglich. Somit werden diese vor unbefugter Manipulation geschützt.

Z.Zeit-Ort Das System kann den Zugang in Abhängigkeit vom jeweiligen Benutzer auf bestimmte Zeitpunkte und Zugangspunkte beschränken.

Z.Umgehung Das System stellt sicher, daß Angreifer mittels vorsätzlich manipulierter oder fehlerhafter Software die Sicherheitsmechanismen des Systems, unter Berücksichtigung des angenommenen Angriffspotentials, nicht

umgehen können.

Z.Fehler	Das System enthält keine für Angriffe auf die IT-Sicherheit des Systems ausnutzbaren Schwachstellen, unter Berücksichtigung des angenommenen Angriffspotentials, in Design, Implementierung oder Betrieb.
Z.SysAdmin	Das System stellt alle erforderlichen Funktionen für seine Verwaltung durch berechtigte Systemadministratoren zur Verfügung.
Z.Betrieb	Das System gewährleistet die fortlaufende korrekte Funktionsweise seiner Sicherheitsfunktionen.
Z.Status	Das System gewährleistet jederzeit die Überprüfung seines Sicherheitsstatus durch die dazu befugten Systemadministratoren.
Z.Verfügbarkeit	Das System gewährleistet die durchgehende Verfügbarkeit seiner Ressourcen für seine befugten Benutzer.
Z.Zustand	Das System bewahrt auch im Fehlerfall einen sicheren Zustand.
Z.Verbindung	Das System kann mit vertrauenswürdigen Partnern unter Erhalt der Vertraulichkeit und Integrität der übertragenen Daten kommunizieren.
Z.Software	Die auf den Systemen in sicherheitsrelevanten Bereichen zum Einsatz kommende Software ist vertrauenswürdig. Dies wird dadurch erreicht, daß sie methodisch entwickelt, getestet und durchgesehen wurde.

5.2 Sicherheitsziele für die Umgebung

Z.Installation	Die für den Betrieb des Systems Verantwortlichen stellen sicher, daß das System in einer Art und Weise ausgeliefert und installiert wird, die die Sicherheit des Systems gewährleistet.
Z.Definition	Die Definition und Zuweisung von Rollen und Gruppen erfolgt in Übereinstimmung mit der geltenden Sicherheitspolitik. Aufgaben und die von einem berechtigten Benutzer zu einem bestimmten Zeitpunkt ausgeübte Rolle sind jederzeit klar erkennbar.
Z.Geheim	Die Benutzer gewährleisten den Schutz ihrer Authentisierungsgeheimnisse.
Z.Aufbewahrung	In der Betriebsumgebung bestehen Möglichkeiten zur Aufbewahrung von Daten, Programmen und Protokollinformationen gemäß den gesetzlichen Regelungen.
Z.KommAdmin	Die für den Betrieb des Systems Verantwortlichen stellen sicher, daß keine Verbindungen zu nicht vertrauenswürdigen Systemen die Sicherheit des Systems gefährden.

Hinzu kommen die Sicherheitsziele, die sich durch eine direkte Umsetzung der Annahmen aus Abschnitt 4.1 ergeben. Diese Sicherheitsziele werden dementsprechend z.B. als Z.SiPol in direkter Umsetzung von A.SiPol bezeichnet:

Z.Zutritt	Einige, jedoch nicht notwendigerweise alle Betriebsmittel des Systems, einschließlich der Arbeitsplätze, befinden sich innerhalb kontrollierter Räumlichkeiten, zu denen nicht befugten Personen der Zugang verwehrt wird.
Z.Schutz	Sämtliche Systemkomponenten, die wesentlich zur Durchsetzung der

Sicherheitspolitik sind und die nicht selbst über Vorrichtungen zum Schutz vor unbefugten materiellen Eingriffen und Modifikationen verfügen, werden durch geeignete materielle Maßnahmen vor Eingriffen und Modifikationen durch unbefugte Dritte geschützt.

Z.Admin Es gibt eine oder mehrere ausgebildete Personen, die das System verwalten, einschließlich der Sicherheit der darin verarbeiteten Informationen und der Zuweisung der Betriebsmittel. Diese Personen sind im Rahmen der ihnen übertragenen Aufgaben als vertrauenswürdig zu betrachten.

Z.Benutzer Die Benutzer sind für die ihnen übertragenen Aufgaben ausreichend geschult, um die Sicherheitsfunktionen des Systems, soweit sie von ihnen benutzt werden, korrekt und in Übereinstimmung mit der Sicherheitspolitik anzuwenden.

Z.Partner Andere Systeme, mit denen ein SIZ-PP-konformes System kommuniziert, unterliegen der gleichen administrativen Kontrolle und werden unter der gleichen Sicherheitspolitik betrieben wie das System selbst.

Z.SiPol Die organisatorischen und personellen Anteile der in Abschnitt 4.3 „Organisatorische Sicherheitspolitiken“ beschriebenen Sicherheitspolitik werden im Unternehmen mit Unterstützung des Managements umgesetzt.

6 IT-Sicherheitsanforderungen

6.1 Funktionale Sicherheitsanforderungen an den EVG

Hinweis: Sofern eine der von den CC erlaubten Operationen Zuweisung, Auswahl, Iteration und Verfeinerung auf einer der ausgewählten funktionalen Komponenten ausgeführt wurde, so ist das Ergebnis der ausgeführten Operation durch eine graue Text-Hinterlegung deutlich gemacht.

6.1.1 Tabellarische Übersicht

Funktionale Sicherheits-anforderung	Bezeichnung
FIA	**Identifikation und Authentisierung**
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
FIA_USB.1	Benutzer-Subjekt-Bindung
FIA_ATD.1	Definition der Benutzerattribute
FIA_UAU.2	Benutzerauthentisierung vor jeglicher Aktion
FIA_UAU.4	Authentisierungsmechanismus für einmaligen Gebrauch
FIA_UAU.5	Mehrfache Authentisierungsmechanismen
FIA_UAU.6	Wiederauthentisierung
FIA_UAU.7	Geschützte Authentisierungsrückmeldung
FIA_SOS.1	Verifizierung von Geheimnissen
FIA_AFL.1	Handhabung von Authentisierungsfehlern
FTA	**EVG-Zugriff**
FTA_TSE.1	EVG-Sitzungseinrichtung
FTA_LSA.1	Begrenzung des Anwendungsbereiches der auswählbaren Attribute
FTA_SSL.1	Durch TSF eingeleitetes Sperren der Sitzung
FTA_SSL.2	Durch Benutzer eingeleitetes Sperren
FTA_MCS.1	Einfache Begrenzung bei mehreren gleichzeitigen Sitzungen
FTA_TAH.1	EVG-Zugriffshistorie
FDP	**Schutz der Benutzerdaten**
FDP_ACC.1	Teilweise Zugriffskontrolle
FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen
FDP_SDI.2	Überwachung der Integrität der gespeicherten Daten und

Funktionale Sicherheits-anforderung	Bezeichnung
	Reaktionen
FDP_UCT.1	Einfache Vertraulichkeit des Datenaustausches
FDP_UIT.1	Einfache Integrität des Datenaustausches
FDP_RIP.2	Vollständiger Schutz bei erhalten gebliebenen Informationen
FPT	**Schutz der EVG-Sicherheitsfunktionen**
FPT_PHP.3	Widerstand gegen materielle Angriffe
FPT_RVM.1	Nichtumgehbarkeit der TSP
FPT_SEP.2	SFP Bereichsseparierung
FPT_AMT.1	Test der abstrakten Maschine
FPT_TST.1	TSF testen
FPT_FLS.1	Erhaltung des sicheren Zustandes bei Fehlern
FPT_RCV.1	Manuelle Wiederherstellung
FPT_ITA.1	Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik
FPT_ITC.1	Vertraulichkeit bei Inter-TSF-Datenübertragung
FPT_ITI.1	Inter-TSF-Erkennung von Modifizierungen
FPT_RPL.1	Erkennen von Wiedereinspielung
FPT_STM.1	Verläßliche Zeitstempel
FCO	**Kommunikation**
FCO_NRO.1	Selektiver Urheberschaftsbeweis
FCO_NRR.1	Selektiver Empfangsbeweis
FTP	**Vertrauenswürdiger Pfad/Kanal**
FTP_TRP.1	Vertrauenswürdiger Pfad
FTP_ITC.1	Inter-TSF Vertrauenswürdiger Kanal
FCS	**Kryptographische Unterstützung**
FCS_COP.1	Kryptographischer Betrieb
FCS_CKM.1	Generierung des kryptographischen Schlüssels
FCS_CKM.2	Verteilung des kryptographischen Schlüssels
FCS_CKM.3	Zugriff auf den kryptographischen Schlüssel
FCS_CKM.4	Zerstörung des kryptographischen Schlüssels
FAU	**Sicherheitsprotokollierung**

Funktionale Sicherheits-anforderung	Bezeichnung
FAU_GEN.1	Generierung der Protokolldaten
FAU_GEN.2	Verknüpfung der Benutzeridentität
FAU_SEL.1	Auswahl der Ereignisse für die Sicherheitsprotokollierung
FAU_SAA.1	Analyse von möglichen Verletzungen
FAU_ARP.1	Sicherheitsalarme
FAU_STG.2	Garantie der Verfügbarkeit der Protokolldaten
FAU_STG.4	Schutz vor Protokolldaten-Verlust
FAU_SAR.1	Durchsicht der Protokollierung
FAU_SAR.2	Eingeschränkte Durchsicht der Protokollierung
FAU_SAR.3	Auswählbare Durchsicht der Protokollierung
FMT	**Sicherheitsmanagement**
FMT_MOF.1	Management des Verhaltens der Sicherheitsfunktionen
FMT_MSA.1	Management der Sicherheitsattribute
FMT_MSA.2	Sichere Sicherheitsattribute
FMT_MSA.3	Initialisierung statischer Attribute
FMT_MTD.1	Management der TSF-Daten
FMT_MTD.2	Management der Begrenzungen für TSF-Daten
FMT_REV.1	Widerruf
FMT_SAE.1	Zeitlich begrenzte Autorisierung
FMT_SMR.1	Sicherheitsrollen
FMT_SMR.2	Einschränkungen der Sicherheitsrollen
FMT_SMR.3	Annahme von Rollen

Tabelle 1: Funktionale Sicherheitsanforderungen

6.1.2 Identifikation und Authentisierung (FIA)

Erläuterung: Eine weit verbreitete Sicherheitsanforderung ist es, die Person und/oder Einheit eindeutig zu identifizieren, die in einem EVG Funktionen ausführt. Das beinhaltet nicht nur, die angegebene Identität eines jeden Benutzers festzustellen, sondern auch zu verifizieren, daß jeder Benutzer tatsächlich derjenige ist, für den er sich ausgibt. Das wird dadurch erreicht, daß die Benutzer den TSF einige mit den entsprechenden Benutzern verknüpfte Informationen liefern müssen.

Die Familien dieser Klasse betreffen die Anforderungen an Funktionen zur Feststellung und Verifizierung postulierter Benutzeridentitäten. Identifikation

und Authentisierung sind erforderlich um sicherzustellen, daß die Benutzer mit den ordnungsgemäßen Sicherheitsattributen verknüpft werden (zum Beispiel Identität, Gruppe, Rolle, Sicherheits- oder Integritätsstufen).

Die eindeutige Identifikation von autorisierten Benutzern und die korrekte Verknüpfung von Sicherheitsattributen mit Benutzern und Subjekten ist entscheidend für die Durchsetzung der Sicherheitspolitiken.

6.1.2.1 Benutzeridentifikation (FIA_UID)

Erläuterung: Diese Familie definiert die Bedingungen, unter denen von den Benutzern gefordert wird, sich vor Ausführung irgendwelcher anderer von den TSF vermittelten und eine Benutzeridentifikation erfordernden Aktionen zu identifizieren.

FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

Erläuterung: FIA_UID.2 erfordert von den Benutzern, daß diese sich identifizieren, bevor die TSF jegliche Aktion gestatten.

FIA_UID.2.1 Die TSF müssen erfordern, daß sich jeder Benutzer identifiziert, bevor für diesen Benutzer jegliche andere TSF-vermittelte Aktionen erlaubt werden.

6.1.2.2 Benutzer-Subjekt-Bindung (FIA_USB)

Erläuterung: Ein authentisierter Benutzer aktiviert in der Regel ein Subjekt, um den EVG zu benutzen. Die Benutzersicherheitsattribute sind (vollständig oder teilweise) mit dem Subjekt verknüpft. Diese Familie definiert Anforderungen zur Erzeugung und Erhaltung der Verknüpfung der Benutzersicherheitsattribute mit dem Subjekt, das für den Benutzer handelt.

FIA_USB.1 Benutzer-Subjekt-Bindung

Erläuterung: FIA_USB.1 Benutzer-Subjekt-Bindung erfordert die Erhaltung der Verknüpfung zwischen den Sicherheitsattributen des Benutzers und einem Subjekt, das für den Benutzer handelt.

FIA_USB.1.1 Die TSF müssen die angemessenen Benutzersicherheitsattribute mit den Subjekten verknüpfen, die für die Benutzer handeln.

Verfeinerung:

Als Minimum sind dem Subjekt folgende Benutzerattribute zuzuordnen:

- die eindeutige Benutzerkennung, über die es möglich ist, statische Sicherheitsattribute, die zu dieser Kennung gehören, bei Bedarf nachzuschlagen.
- dynamische Attribute, die sich zur Laufzeit oder pro Sitzung ändern können.

6.1.2.3 Definition der Benutzerattribute (FIA_ATD)

Erläuterung: Alle autorisierten Benutzer können eine die Benutzeridentität nicht mit einschließende Menge von Sicherheitsattributen besitzen, die zur Durchsetzung der TSP genutzt werden. Diese Familie definiert die Anforderungen an das Verknüpfen von Benutzersicherheitsattributen mit Benutzern entsprechend den Erfordernissen zur Unterstützung der TSP.

FIA_ATD.1 Definition der Benutzerattribute

Erläuterung: FIA_ATD.1 erlaubt für jeden Benutzer die individuelle Erhaltung der Benutzersicherheitsattribute.

FIA_ATD.1.1 Die TSF müssen die folgende Liste von Sicherheitsattributen, die zu einzelnen Benutzern gehören, erhalten:

- einen vollen Namen oder andere Informationen, die einen eindeutigen Rückschluß auf die tatsächliche Person bzw. den Kommunikationspartner zulassen
- eine Liste der Gruppen, denen der Benutzer angehört
- eine Liste der Rollen, denen der Benutzer angehört
- die Attribute zur Konfiguration des Systemzuganges
- die Lebensdauer der Kennung
- die erlaubten Login-Zeiten
- den Zeitpunkt des letzten erfolgreichen Logins, den Zeitpunkt des letzten fehlgeschlagenen Logins und die Anzahl der aufeinanderfolgenden fehlgeschlagenen Logins
- eine Liste der erlaubten Zugangspunkte
- die Attribute zur Konfiguration des Authentisierungsmechanismus:
  - die Attribute des Authentisierungsgeheimnisses
  - die individuellen Attribute für Parameter des Authentisierungsmechanismus. Bei regelmäßig zu ändernden Authentisierungsgeheimnissen wie Paßwörtern oder PINs sind dies:
    - der Zeitpunkt der letzten Änderung oder die Anzahl der Änderungen an einem Tag
    - das Verfallsdatum
    - der Zeitpunkt der Warnung über die bevorstehende Änderung
    - eine Liste der zuletzt verwendeten Authentisierungsgeheimnisse. Die Länge dieser Liste muß dabei ein Mehrfaches der pro Tag zulässigen Änderungen des Authentisierungsgeheimnisses betragen.

6.1.2.4 Benutzerauthentisierung (FIA_UAU)

Erläuterung: Diese Familie definiert die von den TSF unterstützten Arten von Benutzerauthentisierungsmechanismen. Diese Familie definiert ebenfalls die geforderten Attribute, auf denen die Benutzerauthentisierungsmechanismen basieren müssen.

FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion

Erläuterung: FIA_UAU.2 erfordert, daß Benutzer sich authentisieren, bevor von den TSF jegliche Aktion erlaubt wird.

FIA_UAU.2.1 Die TSF müssen erfordern, daß jeder Benutzer erfolgreich authentisiert wird, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FIA_UAU.4 Authentisierungsmechanismus für einmaligen Gebrauch

Erläuterung: FIA_UAU.4 erfordert einen Authentisierungsmechanismus, der mit Authentisierungsdaten für einmaligen Gebrauch arbeitet.

FIA_UAU.4.1 Die TSF müssen den Wiedergebrauch von Authentisierungsdaten, die mit dem Authentisierungsmechanismus „starke Authentisierung“ in Beziehung stehen, verhindern.

FIA_UAU.5 **Mehrfache Authentisierungsmechanismen**

Erläuterung: FIA_UAU.5 erfordert, daß verschiedene Authentisierungsmechanismen bereitgestellt und zum Authentisieren von Benutzeridentitäten für spezielle Ereignisse benutzt werden.

FIA_UAU.5.1 Die TSF müssen folgende Authentisierungsmechanismen zur Unterstützung der Benutzerauthentisierung bereitstellen:

- „keine Authentisierung“
- „paßwortbasierte Authentisierung“ oder ein mindestens gleich starker Authentisierungsmechanismus.
- „Starke Authentisierung“ nach Anforderung FIA_UAU.4, falls Zugänge nicht-anonymer Benutzer zum System über externe, ungeschützte Leitungen erfolgen.
- „Mehraugen-Prinzip“[6]
- Zusätzliche Authentisierungsmechanismen, die befugte Systemadministratoren installieren können.

FIA_UAU.5.2 Die TSF müssen jede von einem Benutzer angegebene Identität gemäß den folgenden Regeln authentisieren:

- Systeme, die Informationsdienste für anonyme Benutzer zur Verfügung stellen, verwenden für solche anonymen Benutzer den Mechanismus „keine Authentisierung“.
- Alle anderen Benutzer verwenden beim Zugang über interne Netze und über geschützte externe Leitungen mindestens den Mechanismus „paßwortbasierte Authentisierung“ oder sein Äquivalent.
- Alle Benutzer, die Zugang zum System über ungeschützte externe Leitungen erhalten wollen, benutzen den Mechanismus „Starke Authentisierung“.
- Der Zugang unter besonders sicherheitskritischen Kennungen soll über den Mechanismus „Mehraugen-Prinzip“ erfolgen.

[6] Unter das Mehraugen-Prinzip fällt das Vier-Augen-Prinzip als Spezialfall. Allgemein sind damit Verfahren gemeint, bei denen m von n Personen zustimmen müssen, mit $m \geq 2$ und $m \leq n$.

Verfeinerung:

Der befugte Systemadministrator soll festlegen können, ob die zusätzlich installierten Authentisierungsmechanismen anstatt der oder zusätzlich zu den bisher vorhandenen Authentisierungsmechanismen benutzt werden sollen.

FIA_UAU.6 **Wiederauthentisierung**

Erläuterung: FIA_UAU.6 erfordert die Fähigkeit zur Spezifikation von Ereignissen, für die der Benutzer wiederauthentisiert werden muß.

FIA_UAU.6.1 Die TSF müssen den Benutzer unter den Bedingungen

- Ausbleiben von Ein- bzw. Ausgaben an dem Endgerät während einer aktiven Sitzung über eine in Übereinstimmung mit der Sicherheitspolitik einstellbaren Zeit
- Änderung der Authentisierungsdaten durch den Benutzer (z.B. Wechsel des Paßwortes)
- Anforderung durch eine Anwendung über eine vom System bereitgestellte Programmierschnittstelle

wiederauthentisieren.

FIA_UAU.7 **Geschützte Authentisierungsrückmeldung**

Erläuterung: FIA_UAU.7 erfordert, daß während der Authentisierung dem Benutzer nur begrenzte Rückmeldungsinformationen bereitgestellt werden.

FIA_UAU.7.1 Die TSF müssen sicherstellen, daß während der Authentisierung nur Rückmeldungen, die keinerlei Rückschlüsse auf evtl. eingegebene Authentisierungsgeheimnisse erlauben, an den Benutzer bereitgestellt werden.

6.1.2.5 Spezifikation der Geheimnisse (FIA_SOS)

Erläuterung: Diese Familie definiert Anforderungen an Mechanismen, die definierte Qualitätsmetriken für gegebene Geheimnisse durchsetzen und Geheimnisse generieren, die die definierte Metrik erfüllen.

FIA_SOS.1 **Verifizierung von Geheimnissen**

Erläuterung: FIA_SOS.1 erfordert von den TSF eine Verifizierung, daß die Geheimnisse definierte Qualitätsmetriken erfüllen.

FIA_SOS.1.1 Die TSF müssen einen Mechanismus bereitstellen, um zu verifizieren, daß die Geheimnisse den folgenden Anforderungen

- Neu gewählte Authentisierungsgeheimnisse müssen sich von dem zu diesem Zeitpunkt für diesen Benutzer gültigen Authentisierungsgeheimnis unterscheiden.
- Neu gewählte Authentisierungsgeheimnisse dürfen in der Liste der zuletzt von diesem Benutzer verwendeten Authentisierungsgeheimnisse nicht enthalten sein.
- Bei der Benutzung von Mechanismen für wiederverwendbare Paßwörter als Authentisierungsgeheimnis sollen zusätzlich folgende Richtlinien gelten:

  - Paßwörter müssen eine Mindestlänge von sechs Zeichen haben und sich aus Buchstaben, Ziffern und Sonderzeichen zusammensetzen.
  - Paßwörter müssen mindestens ein Zeichen enthalten, das kein Buchstabe ist.
  - Triviale Paßwörter müssen über Ausnahmelisten vermieden werden können.
  - Der Mechanismus zur Paßwortüberprüfung muß austauschbar sein.
- Bei Nichterfüllung einer der o.g. Anforderungen wird eine Änderung des zu diesem Zeitpunkt für diesen Benutzer gültigen Authentisierungsgeheimnisses abgewiesen.

entsprechen.

6.1.2.6 Authentisierungsfehler (FIA_AFL)

Erläuterung: Diese Familie enthält Anforderungen zum Definieren von Werten für eine Anzahl von Authentisierungsversuchen und TSF-Aktionen für den Fall, daß Authentisierungsversuche mißlingen. Die Parameter enthalten u.a. die Anzahl der mißlungenen Authentisierungsversuche und Zeitschwellen.

FIA_AFL.1 **Handhabung von Authentisierungsfehlern**

Erläuterung: FIA_AFL.1 erfordert, daß die TSF in der Lage sein müssen, den Prozeß der Sitzungseinrichtung nach einer spezifizierten Anzahl von mißlungenen Benutzerauthentisierungsversuchen zu beenden. Sie erfordert auch, daß die TSF nach Beendigung des Sitzungseinrichtungsprozesses in der Lage sein müssen, die Benutzerkennung oder den Zugangspunkt (zum Beispiel Workstation), von dem die Versuche unternommen wurden, bis zum Auftreten einer vom Systemadministrator definierten Bedingung zu deaktivieren.

FIA_AFL.1.1 Die TSF müssen erkennen, wenn hintereinander mindestens drei mißlungene Authentisierungsversuche auftreten, die in Bezug zu

- der Eingabe eines Benutzernamens,
- der Eingabe eines Authentisierungsgeheimnisses,

stehen.

FIA_AFL.1.2 Wenn die definierte Anzahl von fehlgeschlagenen Authentisierungsversuchen erreicht oder überschritten wird, müssen die TSF

- einen befugten Systemadministrator benachrichtigen,
- bei wiederholten Fehlversuchen unter einer Benutzerkennung diese Benutzerkennung bis zu einer erneuten Freigabe durch einen befugten Systemadministrator sperren,
- bei wiederholten Fehlversuchen von einem Zugangspunkt diesen Zugangspunkt bis zu einer erneuten Freigabe durch einen befugten Systemadministrator sperren.

6.1.3 EVG-Zugriff (FTA)

Erläuterung: Diese Klasse spezifiziert funktionale Anforderungen zur Kontrolle der Einrichtung einer Benutzersitzung.

6.1.3.1 EVG-Sitzungseinrichtung (FTA_TSE)

Erläuterung: Diese Familie definiert Anforderungen zum Verweigern der Erlaubnis für einen Benutzer, eine Sitzung mit dem EVG einzurichten.

FTA_TSE.1 **EVG-Sitzungseinrichtung**

Erläuterung: FTA_TSE.1 stellt Anforderungen bereit, mit denen Benutzern der auf Attributen basierende Zugriff auf den EVG verweigert wird.

FTA_TSE.1.1 Die TSF müssen in der Lage sein, basierend auf

- dem Zeitpunkt der Anforderung einer Sitzungseinrichtung,
- dem Zugangspunkt, von dem aus eine Sitzungseinrichtung angefordert wird,
- der Benutzerkennung, für die eine Sitzungseinrichtung angefordert wird

eine Sitzungseinrichtung zu verweigern.

6.1.3.2 Begrenzung des Anwendungsbereiches der auswählbaren Attribute (FTA_LSA)

Erläuterung: Diese Familie definiert Anforderungen zur Begrenzung des Anwendungsbereichs von Sitzungs-Sicherheitsattributen, die ein Benutzer für eine Sitzung auswählen kann.

FTA_LSA.1 **Begrenzung des Anwendungsbereiches der auswählbaren Attribute**

Erläuterung: FTA_LSA.1 stellt die Anforderung bereit, daß ein EVG den Anwendungsbereich der Sitzungs-Sicherheitsattribute während der Sitzungseinrichtung begrenzt.

Als einziges wählbares Sicherheitsattribut wird die Rolle des Benutzers festgelegt.

FTA_LSA.1.1 Die TSF müssen den Anwendungsbereich der Sitzungs-Sicherheitsattribute „Auswahl einer Rolle“ basierend auf

- dem Zeitpunkt des Zuganges,
- dem Ort des Zuganges,
- der Art des Zuganges,
- einer Liste anderer ausgewählter Rollen

einschränken.

Verfeinerung:

Insbesondere soll es möglich sein, daß bestimmte Rollen nur exklusiv eingenommen werden dürfen.

6.1.3.3 Sperren der Sitzung (FTA_SSL)

Erläuterung: Diese Familie definiert Anforderungen an die TSF, die Fähigkeit des durch TSF und Benutzer eingeleiteten Sperrens und Entsperrens von interaktiven Sitzungen bereitzustellen.

FTA_SSL.1 **Durch TSF eingeleitetes Sperren der Sitzung**

Erläuterung: FTA_SSL.1 schließt ein vom System eingeleitetes Sperren einer interaktiven Sitzung nach einer spezifizierten Zeitspanne von Benutzerinaktivität ein.

FTA_SSL.1.1 Die TSF müssen eine interaktive Sitzung nach Ablauf einer in Übereinstimmung mit der Sicherheitspolitik einstellbaren Zeitspanne ohne Benutzeraktivität sperren, und zwar durch:

- Löschen oder Überschreiben von Anzeigegeräten, wobei die gegenwärtigen Inhalte unlesbar gemacht werden
- Deaktivierung aller Aktivitäten von Zugriffs-/Anzeigegeräten außer dem Entsperren der Sitzung.

FTA_SSL.1.2 Die TSF müssen das Eintreten folgender Ereignisse vor dem Entsperren der Sitzung erfordern:

- Der dieser Sitzung zugeordnete Benutzer muß vom System erneut authentisiert worden sein.

FTA_SSL.2 **Durch Benutzer eingeleitetes Sperren**

Erläuterung: FTA_SSL.2 stellt Fähigkeiten bereit, mit denen der Benutzer die eigenen interaktiven Sitzungen sperren und entsperren kann.

FTA_SSL.2.1 Die TSF müssen ein durch Benutzer eingeleitetes Sperren der eigenen interaktiven Sitzung des Benutzers zulassen, und zwar durch:

- Löschen oder Überschreiben von Anzeigegeräten, wobei die gegenwärtigen Inhalte unlesbar gemacht werden
- Deaktivierung aller Aktivitäten von Zugriffs-/Anzeigegeräten außer dem Entsperren der Sitzung.

FTA_SSL.2.2 Die TSF müssen das Eintreten folgender Ereignisse vor dem Entsperren der Sitzung erfordern:

- Der dieser Sitzung zugeordnete Benutzer muß vom System erneut authentisiert worden sein.

6.1.3.4 Begrenzung bei mehreren gleichzeitigen Sitzungen (FTA_MCS)

Erläuterung: Diese Familie definiert Anforderungen zur Begrenzung der Anzahl gleichzeitiger, zum selben Benutzer gehörender Sitzungen.

FTA_MCS.1 **Einfache Begrenzung bei mehreren gleichzeitigen Sitzungen**

Erläuterung: FTA_MCS.1 stellt Begrenzungen bereit, die alle Benutzer der TSF betreffen.

FTA_MCS.1.1 Die TSF müssen die maximale Anzahl von gleichzeitigen, zum selben Benutzer gehörenden Sitzungen einschränken.

Verfeinerung:
Die Obergrenze für gleichzeitige Sitzungen soll systemweit oder benutzerspezifisch festgelegt werden können.

FTA_MCS.1.2 Die TSF müssen als Standardvorgabe eine Begrenzung auf maximal eine Sitzung pro Benutzer durchsetzen.

6.1.3.5 EVG-Zugriffshistorie (FTA_TAH)

Erläuterung: FTA_TAH definiert Anforderungen, daß die TSF einem Benutzer nach erfolgreicher Sitzungseinrichtung eine Historie der erfolgreichen und mißlungenen Zugriffsversuche auf den Benutzeraccount anzeigen.

FTA_TAH.1 **EVG-Zugriffshistorie**

Erläuterung: FTA_TAH.1 stell die Anforderungen bereit, mit denen ein EVG Informationen anzeigt, die mit früheren Versuchen, eine Sitzung einzurichten, in Beziehung stehen.

FTA_TAH.1.1 Nach erfolgreicher Sitzungseinrichtung müssen die TSF dem Benutzer Datum, Zeit und Ort der letzten erfolgreichen Sitzungseinrichtung anzeigen.

FTA_TAH.1.2 Nach erfolgreicher Sitzungseinrichtung müssen die TSF dem Benutzer Datum, Zeit und Ort des letzten mißlungenen Versuchs einer Sitzungseinrichtung und die Anzahl von mißlungenen Versuchen seit der letzten erfolgreichen Sitzungseinrichtung anzeigen.

FTA_TAH.1.3 Die TSF müssen sicherstellen, die Informationen der Zugriffshistorie von der Benutzerschnittstelle nicht zu löschen, ohne dem Benutzer die Möglichkeit zur Durchsicht der Informationen zu geben.

6.1.4 Schutz der Benutzerdaten (FDP)

Erläuterung: Diese Klasse enthält Familien, welche die Anforderungen an EVG-Sicherheitsfunktionen und EVG-Sicherheitsfunktionspolitiken spezifizieren, die in Bezug zum Schutz der Benutzerdaten stehen.

Zum Schutz der Benutzerdaten werden in diesem Schutzprofil nur Funktionen der Zugriffskontrolle festgelegt. Es gibt keine Anforderungen für eine Informationsflußkontrolle.

Bei der Zugriffskontrolle wird zwischen einer benutzerbestimmten Zugriffskontrolle und einer rollenbasierten Zugriffskontrolle unterschieden.

Für die benutzerbestimmte Zugriffskontrolle wird festgesetzt, daß sie für das betrachtete Gesamtsystem gelten soll, während die rollenbasierte Zugriffskontrolle innerhalb eines geschützten, in sich abgeschlossenen Subsystems von Anwendungen gewährleistet sein soll.

6.1.4.1 Benutzerbestimmte Zugriffskontrolle (DAC)

Erläuterung: Die benutzerbestimmte Zugriffskontrolle (Discretionary Access Control – DAC) stellt die Minimalanforderung für eine Zugriffskontrolle auf Objekte dar, die durch das Betriebssystem kontrolliert werden. Die benutzerbestimmte Zugriffskontrolle muß so einsetzbar sein, daß sie auch den unten beschriebenen RBAC-Mechanismus schützen kann.

6.1.4.1.1 Benutzerbestimmte Zugriffskontrollpolitik (FDP_ACC - DAC)

Erläuterung: Diese Familie identifiziert SFPs für Zugriffskontrolle (DAC) und definiert den Anwendungsbereich der Kontrolle der Politiken, die den identifizierten Teil der Zugriffskontrolle der TSP bilden. Dieser Anwendungsbereich der Kontrolle wird durch drei Mengen charakterisiert: die Subjekte unter Kontrollpolitik, die Objekte unter Kontrollpolitik und die Operationen zwischen kontrollierten Subjekten und kontrollierten Objekten, die durch die Politik abgedeckt sind.

FDP_ACC.1 **Teilweise Zugriffskontrolle**

Erläuterung: FDP_ACC.1 erfordert, daß jede identifizierte SFP für Zugriffskontrolle für eine Teilmenge der möglichen Operationen mit einer Teilmenge der Objekte eines EVG angewendet wird.

FDP_ACC.1.1 (DAC) Die TSF müssen die benutzerbestimmte Zugriffskontrolle für die Zugriffe von

- allen Subjekten auf
- Objekte im Sinne der benutzerbestimmten Zugriffskontrolle

durchsetzen.

Verfeinerung:
Objekte im Sinne der benutzerbestimmten Zugriffskontrolle sind

- alle persistenten Objekte
- Objekte der Interprozeßkommunikation

6.1.4.1.2 Zugriffskontrollfunktionen (FDP_ACF - DAC)

Erläuterung: Diese Familie beschreibt die Regeln für die besonderen Funktionen, die eine in FDP_ACC genannte Politik für Zugriffskontrolle implementieren können, die auch den Anwendungsbereich der Kontrolle der Politik spezifiziert.

FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

Erläuterung: FDP_ACF.1 erlaubt den TSF, den Zugriff basierend auf Sicherheitsattributen und genannten Gruppen von Attributen durchzusetzen. Außerdem können die TSF die Fähigkeit haben, basierend auf Sicherheitsattributen, den Zugriff auf ein Objekt explizit zu autorisieren oder zu verweigern.

FDP_ACF.1.1 (DAC) Die TSF müssen die benutzerbestimmte Zugriffskontrolle für Objekte, die auf den folgenden Attributen basieren, durchsetzen:

Subjektattribute:

- die Benutzerkennung des Subjektes
- eine Liste der Gruppen, in denen der Benutzer Mitglied ist
- die Privilegien des Subjekts, soweit vom System unterstützt.

Objektattribute (Zugriffskontrollisten – Access Control Lists (ACLs)):

- eine Liste von Benutzer- und/oder Gruppenkennungen, sowie für jeden Listeneintrag eine Liste der erlaubten Operationen.
- eine Liste von Benutzer- und/oder Gruppenkennungen, für die jeder Zugriff explizit verboten ist
  und/oder
- eine Liste von Benutzer- und/oder Gruppenkennungen, sowie für jeden Listeneintrag eine Liste der explizit verbotenen Operationen

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

- Die Benutzerkennung ist nicht in der Liste der Benutzerkennungen vorhanden, für die der Zugriff explizit verboten ist.
- Keine der Gruppen aus der Liste der Gruppen des Subjekts ist in der Liste der Gruppen vorhanden, für die der Zugriff explizit verboten ist.
- Die (kumulierten) Rechte aus den ACL-Einträgen, die die Benutzerkennung oder mindestens eine der Gruppen aus der Gruppenliste des Subjektes enthalten, beinhalten alle angeforderten Zugriffsrechte.

FDP_ACF.1.3 (DAC) Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf den folgenden zusätzlichen Regeln, explizit autorisieren:

- Zugriffsverweigerung hat Vorrang vor der Gewährung des Zugriffs. Der befugte Systemadministrator darf alle für ihn zugelassenen Operationen auf alle Objekte durchführen[7]

FDP_ACF.1.4 (DAC) Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf folgenden Regeln:

- Die Benutzerkennung ist in der Liste der Benutzerkennungen vorhanden, für die der Zugriff explizit verboten ist.
- Mindestens eine Gruppe aus der Liste der Gruppen des Subjekts ist in der Liste der Gruppen vorhanden, für die der Zugriff explizit verboten ist.

explizit verweigern.

6.1.4.2 Rollenbasierte Zugriffskontrolle (RBAC)

Erläuterung: Sowohl in Fachanwendungen wie auch in der Systemverwaltung werden Rechte und Privilegien auf der Basis eines Rollenkonzeptes vergeben. Während die rollenbasierte Rechtevergabe und -prüfung für Systemadministratoren durch die Anforderungen nach administrativen Rollen abgedeckt ist, benötigen Fachanwendungen eine rollenbasierte Zugriffskontrolle, die den nachfolgenden Anforderungen gerecht wird.

6.1.4.2.1 Rollenbasierte Zugriffskontrollpolitik (FDP_ACC - RBAC)

Erläuterung: Diese Familie identifiziert SFPs für Zugriffskontrolle (RBAC) und definiert den Anwendungsbereich der Kontrolle der Politiken, die den identifizierten Teil der Zugriffskontrolle der TSP bilden. Dieser Anwendungsbereich der Kontrolle wird durch drei Mengen charakterisiert: die Subjekte unter Kontrollpolitik, die Objekte unter Kontrollpolitik und die Operationen zwischen kontrollierten Subjekten und kontrollierten Objekten, die durch die Politik abgedeckt sind.

FDP_ACC.1 **Teilweise Zugriffskontrolle**

Erläuterung: FDP_ACC.1 erfordert, daß jede identifizierte Zugriffskontroll-SFP für eine Teilmenge der möglichen Operationen mit einer Teilmenge der Objekte eines EVG angewendet wird.

FDP_ACC.1.1 (RBAC) Die TSF müssen die rollenbasierte Zugriffskontrollpolitik (Role Based Access Control - RBAC) für ein abgeschlossenes Teilsystem für jegliche Zugriffe von Subjekten auf die von Fachanwendungen kontrollierten Objekte durchsetzen.

6.1.4.2.2 Zugriffskontrollfunktionen (FDP_ACF - RBAC)

Erläuterung: Diese Familie beschreibt die Regeln für die speziellen Funktionen, die eine der in FDP_ACC genannten Zugriffskontrollpolitiken implementieren können, die auch den Anwendungsbereich der Politikkontrolle spezifiziert.

---

[7] Zugelassene Operationen eines befugten Systemadministrators sind z.B. das Lesen aller Dateien für einen Systemadministrator, der das Recht zum Durchführen von Sicherungen hat.

FDP_ACF.1 **Zugriffskontrolle basierend auf Sicherheitsattributen**

Erläuterung: FDP_ACF.1 erlaubt den TSF den Zugriff basierend auf Sicherheitsattributen und genannten Gruppen von Attributen durchzusetzen. Außerdem können die TSF die Fähigkeit haben, basierend auf Sicherheitsattributen, den Zugriff auf ein Objekt explizit zu autorisieren oder zu verweigern.

FDP_ACF.1.1 (RBAC) Die TSF müssen die rollenbasierte Zugriffskontrolle für Objekte basierend auf den folgenden Attributen durchsetzen:

Subjektattribute:

- die Benutzerkennung
- eine oder mehrere Rollen, die dem Subjekt aus der Menge der für den Benutzer erlaubten Rollen zugewiesen wurden.

Objektattribute:

- eine Liste von Benutzerkennungen und/oder Rollen, die Zugriffsrechte auf das Objekte haben, sowie für jeden Listeneintrag eine Liste der erlaubten Aktionen
- eine Liste von Benutzerkennungen und/oder Rollen, für die ein Zugriff explizit verboten ist.

Weiterhin gibt es eine Hierarchie von Rollen, die angibt, welche Rolle welche anderen Rollen enthält.

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

- Die Benutzerkennung des Subjektes ist nicht explizit in der Liste der Kennungen, für die dieser Zugriff verboten ist.
- Die Liste der Rollen, für die ein Zugriff auf das Objekt explizit verboten ist, enthält keine Rolle, die in der Liste der aktiven Rollen des Subjektes vorkommt oder in einer dieser Rollen enthalten ist.
- Das Subjekt darf auf ein Objekt zugreifen, wenn die Benutzerkennung, unter der das Subjekt agiert, explizit für den Zugriff in der Zugriffskontrolliste des Objektes autorisiert wurde.
- Das Subjekt darf auf ein Objekt zugreifen, wenn in der Liste seiner aktiven Rollen mindestens eine Rolle oder eine in dieser Rolle enthaltene Rolle vorkommt, die in der Zugriffskontrolliste des Objektes für die gewünschte Operation explizit autorisiert ist.

FDP_ACF.1.3 (RBAC) Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf den folgenden zusätzlichen Regeln, explizit autorisieren:

- Die Verweigerung des Zugriffs hat Vorrang vor der Gewährung des Zugriffs

FDP_ACF.1.4 (RBAC) Die TSF müssen den Zugriff von Subjekten auf Objekte, basieren auf folgenden Regeln:

- wenn die Benutzerkennung, unter der das Subjekt agiert, explizit für den Zugriff gesperrt wurde;
- wenn die Liste der Rollen, für die ein Zugriff auf das Objekt explizit verboten ist, eine Rolle enthält, die in der Liste der aktiven Rollen des Subjektes vorkommt oder in einer dieser Rollen enthalten ist;

explizit verweigern.

6.1.4.3 Integrität der gespeicherten Daten (FDP_SDI)

Erläuterung: Diese Familie stellt die Anforderungen bereit, die den Schutz von Benutzerdaten betreffen, während diese innerhalb des TSC gespeichert sind. Integritätsfehler können sich auf gespeicherte Benutzerdaten im Arbeitsspeicher oder in der Speichereinheit auswirken.

FDP_SDI.2 Überwachung der gespeicherten Daten und Reaktionen

Erläuterung: FDP_SDI.2 erfordert, daß die SF die innerhalb des TSC gespeicherten Benutzerdaten auf identifizierte Integritätsfehler überwachen und das Ausführen von Aktionen als Ergebnis einer Fehlererkennung zulassen.

FDP_SDI.2.1 Die TSF müssen die innerhalb des TSC gespeicherten Benutzerdaten auf unbeabsichtigte (z.B. durch fehlerhafte Speichermedien bedingte) Integritätsfehler bei allen Objekten auf Basis folgender Attribute: [Zuweisung: Benutzerdaten- Attribute] überwachen.

FDP_SDI.2.2 Bei Erkennen eines Datenintegritätsfehlers müssen die TSF den Zugriff auf das von diesem Fehler betroffene Objekt mit einem Fehlercode abbrechen.

FDP_SDI.2 Überwachung der gespeicherten Daten und Reaktionen (Iteration)

FDP_SDI.2.1 Die TSF müssen in Systemen mit hohen Verfügbarkeitsanforderungen die innerhalb des TSC gespeicherten Benutzerdaten auf unbeabsichtigte (z.B. durch fehlerhafte Speichermedien bedingte) Integritätsfehler bei allen Objekten auf Basis folgender Attribute: [Zuweisung: Benutzerdaten- Attribute] überwachen und mit hoher Zuverlässigkeit erkennen.

FDP_SDI.2.2 Bei Erkennen eines Datenintegritätsfehlers in Systemen mit hohen Verfügbarkeitsanforderungen müssen die TSF den Zugriff auf das von diesem Fehler betroffene Objekt mit einem Fehlercode abbrechen und die Möglichkeit der automatischen Korrektur des erkannten Fehlers bieten.

6.1.4.4 Schutz der Benutzerdatenvertraulichkeit bei Inter-TSF-Transfer (FDP_UCT)

Erläuterung: Diese Familie definiert die Anforderungen zur Sicherstellung der Vertraulichkeit von Benutzerdaten, wenn diese über einen externen Kanal zwischen unterschiedlichen EVG oder Benutzern in unterschiedlichen EVG übertragen werden.

FDP_UCT.1 Einfache Vertraulichkeit des Datenaustausches

Erläuterung: Das Ziel von FDP_UCT.1 ist die Bereitstellung von Schutz vor Preisgabe der Benutzerdaten während der Übertragung.

FDP_UCT.1.1 Die TSF müssen die benutzerbestimmte Zugriffskontrolle durchsetzen, um in der Lage zu sein, Objekte vor nichtautorisierter Preisgabe geschützt zu übertragen.

6.1.4.5 Schutz der Benutzerdatenintegrität bei Inter-TSF-Transfer (FDP_UIT)

Erläuterung: Diese Familie definiert die Anforderungen an die Integrität der Benutzerdaten während der Übertragung zwischen den TSF und einem anderen vertrauenswürdigen IT-Produkt.

FDP_UIT.1 Einfache Integrität des Datenaustausches

Erläuterung: FDP_UIT.1 betrifft die Erkennung von Modifizierungen, Löschungen, Einfügungen und Wiedereinspielungsfehlern der übertragenen Benutzerdaten.

FDP_UIT.1.1 Die TSF müssen die benutzerbestimmte Zugriffskontrolle durchsetzen, um in der Lage zu sein, Benutzerdaten vor Modifizieren, Löschen, Einfügen und Wiedereinspielen geschützt zu übertragen.

FDP_UIT.1.2 TSF müssen in der Lage sein, beim Empfang der Benutzerdaten festzustellen, ob ein Modifizieren, Löschen, Einfügen oder Wiedereinspielen stattgefunden hat.

6.1.4.6 Schutz bei erhalten gebliebenen Informationen (FDP_RIP)

Erläuterung: Diese Familie betrifft die Notwendigkeit sicherzustellen, daß auf gelöschte Informationen nicht länger zugegriffen werden kann und daß neu erstellte Objekte keine Informationen enthalten, die nicht zugänglich sein sollten. Diese Familie erfordert den Schutz von Informationen, die logisch gelöscht oder freigegeben wurden, sich aber noch innerhalb des EVG befinden können.

FDP_RIP.2 Vollständiger Schutz bei erhalten gebliebenen Informationen

Erläuterung: FDP_RIP.2 Vollständiger Schutz bei erhalten gebliebenen Informationen erfordert von TSF die Sicherstellung, daß jeglicher erhalten gebliebener Informationsinhalt jeglicher Betriebsmittel für alle Objekte bei Zuteilung oder Wiederfreigabe der Betriebsmittel nicht verfügbar ist.

FDP_RIP.2.1 Die TSF müssen sicherstellen, daß der frühere Informationsinhalt eines Betriebsmittels bei Zuteilung eines Betriebsmittels zu allen Objekten nicht verfügbar ist.

6.1.5 Schutz der EVG-Sicherheitsfunktionen (FPT)

Erläuterung: Diese Klasse enthält Familien von funktionalen Anforderungen, die zur Integrität und dem Management der Mechanismen, die die TSF bereitstellen (unabhängig von den TSP-Einzelheiten) und zur Integrität von TSF-Daten (unabhängig vom speziellen Inhalt der TSP-Daten) in Beziehung stehen . Es kann den Anschein haben, daß die Familien dieser Klasse die Komponenten der Klasse FDP (Schutz der Benutzerdaten) duplizieren; diese können sogar mit den gleichen Mechanismen implementiert werden. Dennoch ist FDP auf den Schutz der Benutzerdaten und FPT auf den Schutz der TSF-Daten ausgerichtet. Tatsächlich sind Komponenten der Klasse FPT zur Bereitstellung von Anforderungen erforderlich, damit die SFPs des EVG nicht manipuliert bzw. umgangen werden können.

6.1.5.1 Materieller TSF-Schutz (FPT_PHP)

Erläuterung: Die Anforderungen zum körperlichen Schutz eines Systems beziehen sich auf die Fähigkeit eines Systems, seine logischen Schutzmechanismen dadurch zu schützen, daß es materielle Attacken, die den unbefugten Zugriff auf Informationen oder das Modifizieren der Sicherheitsfunktionen zum Ziel haben, erkennt oder verhindert.

Diese Funktionen werden bei Systemen benötigt, bei denen materielle Attacken als besonderes Risiko angesehen werden (z.B. Geräte, die kryptographische Schlüssel speichern).

FPT_PHP.3 Widerstand gegen materielle Angriffe

Erläuterung: FPT_PHP.3 Widerstand gegen materielle Angriffe stellt Leistungsmerkmale bereit, die materielle Manipulationen von TSF-Geräten und TSF-Elementen verhindern oder diesen widerstehen.

FPT_PHP.3.1 Die TSF müssen [Zuweisung: Szenarien materieller Manipulationen] von [Zuweisung: Liste von TSF-Geräten/Elementen (z.B. Geräten zur Kundenselbstbedienung in unbeaufsichtigten Bereichen wie Geldausgabeautomaten)] widerstehen, indem diese automatisch so reagieren, daß die TSP nicht verletzt wird.

6.1.5.2 Referenzverbindung (FPT_RVM)

Erläuterung: Die Anforderungen dieser Familie betreffen den "immer aktiv"-Aspekt eines herkömmlichen Referenzmonitors. Das Ziel dieser Familie ist es, für eine bestimmte SFP sicherzustellen, daß alle Aktionen, die ein Durchsetzen der Politik erfordern, von den TSF anhand der SFP validiert werden. Falls der Teil der TSF, der die SFP durchsetzt, auch die Anforderungen der angemessenen Komponenten aus FPT_SEP (Bereichsseparierung) und ADV-INT (Interna der EVG-Sicherheitsfunktionen) erfüllt, stellt dieser Teil der TSF einen Referenzmonitor für diese SFP bereit.

FPT_RVM.1 Nichtumgehbarkeit der TSP

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_RVM.1, die eine Nichtumgehbarkeit für alle SFP in der TSP erfordert.

FPT_RVM.1.1 Die TSF müssen sicherstellen, daß die TSF-Funktionen zur Durchsetzung aktiv und erfolgreich sind, bevor den Funktionen innerhalb des TSC die Ausführung gestattet wird.

6.1.5.3 Bereichsseparierung (FPT_SEP)

Erläuterung: Die Komponenten dieser Familie stellen sicher, daß mindestens ein Sicherheitsbereich für die eigene Ausführung der TSF verfügbar ist und daß die TSF gegen externe Eingriffe und Manipulationen (zum Beispiel durch Modifizierung von TSF-Code oder Datenstrukturen) durch nichtvertrauenswürdige Subjekte geschützt sind. Das Erfüllen der Anforderungen dieser Familie machen die TSF selbstschützend. Dies bedeutet, daß ein nichtvertrauenswürdiges Subjekt die TSF nicht modifizieren oder beschädigen kann.

FPT_SEP.2 SFP Bereichsseparierung

Erläuterung: FPT_SEP.2 erfordert eine weitere Unterteilung der TSF: mit einem abgesonderten Bereich bzw. Bereichen für eine identifizierte Menge von SFPs, die als Referenzmonitore für ihre Politiken handeln, und einem Bereich für den Rest der TSF sowie Bereiche für die Teile des EVG, die nicht Teile der TSF sind.

FPT_SEP.2.1 Der nicht getrennte Teil der TSF muß einen Sicherheitsbereich für ihre eigene Ausführung aufrechterhalten, der diese vor Eingriffen und Manipulationen durch nicht vertrauenswürdige Subjekte schützt.

FPT_SEP.2.2 Die TSF müssen die Separierung zwischen den Sicherheitsbereichen von Subjekten im TSC durchsetzen.

FPT_SEP.2.3 Die TSF müssen den Teil der TSF, der zu der benutzerbestimmten Zugriffskontrolle in Beziehung steht, in einem Sicherheitsbereich für deren eigene Ausführung aufrechterhalten, der diese vor Eingriffen und Manipulationen durch den Rest der TSF und durch in Bezug auf diese SFPs nichtvertrauenswürdige Subjekte schützt.

6.1.5.4 Test der zugrundeliegenden abstrakten Maschine (FPT_AMT)

Erläuterung: Diese Familie definiert Anforderungen, daß die TSF Tests zum Nachweis der Sicherheitsannahmen über die zugrundeliegende abstrakte Maschine, auf die sich die TSF verlassen, durchführt. Diese „abstrakte“ Maschine kann eine Hardware- oder Firmwareplattform sein, oder eine anerkannte und bewertete Kombination von Hardware und Software, die als eine virtuelle Maschine agiert.

FPT_AMT.1 Test der abstrakten Maschine

Erläuterung: FPT_AMT.1 stellt das Testen der zugrundeliegenden abstrakten Maschine bereit.

FPT_AMT.1.1 Die TSF müssen beim Erstanlauf, auf Anforderung eines autorisierten Benutzers und nach schweren Ausnahmefehlern eine Testfolge als Nachweis für das korrekte Wirken der Sicherheitsannahmen auf der den TSF zugrundeliegenden abstrakten Maschine durchführen.

6.1.5.5 TSF-Selbsttest (FPT_TST)

Erläuterung: Diese Familie definiert die Anforderungen an den Selbsttest der TSF in Bezug auf einige Operationen, von denen korrektes Wirken erwartet wird. Beispiele sind Schnittstellen zu den Durchsetzungsfunktionen und stichprobenartige arithmetische Operationen in kritischen EVG-Teilen. Diese Tests können während des Anlaufs, in regelmäßigen Abständen, auf Anforderung des autorisierten Benutzers oder bei Zutreffen anderer Bedingungen ausgeführt werden. Die EVG-Aktionen infolge des Selbsttests sind in anderen Familien festgelegt.

FPT_TST.1 TSF testen

Erläuterung: FPT_TST.1 stellt die Fähigkeit zum Testen des korrekten Betriebs der TSF bereit. Diese Tests können beim Anlauf, in regelmäßigen Abständen, auf Anforderungen des autorisierten Benutzers oder bei Zutreffen anderer Bedingungen ausgeführt werden. Sie stellt außerdem die Fähigkeit zur Verifizierung der Integrität von TSF-Daten und ausführbarem Code bereit.

FPT_TST.1.1 Die TSF müssen beim Erstanlauf und auf Anforderung eines autorisierten Benutzers eine Testfolge als Nachweis für den korrekten Betrieb der TSF durchführen.

FPT_TST.1.2 Die TSF müssen für autorisierte Benutzer die Fähigkeit zur Verifizierung der Integrität von TSF-Daten bereitstellen.

FPT_TST.1.3 Die TSF müssen für autorisierte Benutzer die Fähigkeit zur Verifizierung der Integrität von gespeichertem ausführbaren TSF-Code bereitstellen.

6.1.5.6 Sicherer Fehlerzustand (FPT_FLS)

Erläuterung: Die Anforderungen dieser Familie stellen sicher, daß der EVG seine TSP im Fall von TSF-Fehlern identifizierter Kategorien nicht verletzen wird.

FPT_FLS.1 Erhaltung des sicheren Zustandes bei Fehlern

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_FLS.1, die erfordert, daß die TSF bei identifizierten Fehlern einen sicheren Zustand erhalten.

FPT_FLS.1.1 Die TSF müssen den sicheren Zustand bei Auftreten folgender Fehlerarten:

- alle Fehlerarten einschließlich schwerwiegender Ausnahmefehler

erhalten.

6.1.5.7 Vertrauenswürdige Wiederherstellung (FPT_RCV)

Erläuterung: Die Anforderungen dieser Familie stellen sicher, daß die TSF feststellen können, daß der EVG ohne Schutzbloßstellung gestartet wurde und die Wiederherstellung nach Betriebsunterbrechungen ohne Schutzbloßstellung durchführen kann. Diese Familie ist von Bedeutung, weil der Anlaufzustand der TSF den Schutz der Folgezustände bestimmt.

FPT_RCV.1 Manuelle Wiederherstellung

Erläuterung: FPT_RCV.1 erlaubt einem EVG nur die Bereitstellung von Mechanismen, die ein menschliches Eingreifen erfordern, um zu einem sicheren Zustand zurückzukehren.

FPT_RCV.1.1 Nach einem Fehler oder einer Diensteunterbrechung müssen die TSF in einen Erhaltungsmodus wechseln, der die Fähigkeit bereitstellt, den EVG in einen sicheren Zustand zurückzuversetzen.

6.1.5.8 Verfügbarkeit von exportierten TSF-Daten (FPT_ITA)

Erläuterung: Diese Familie definiert die Schutzregeln gegen Verlust der Verfügbarkeit von TSF-Daten, die zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt bewegt werden. Diese Daten können zum Beispiel kritische TSF-Daten wie Paßworte, Schlüssel, Protokolldaten oder ausführbarer TSF-Code sein.

FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_ITA.1. Diese Komponente erfordert, daß die TSF bis zu einem identifizierten Wahrscheinlichkeitsgrad die Verfügbarkeit von TSF-Daten, die für ein entferntes vertrauenswürdiges IT-Produkt bereitgestellt sind, sicherstellen.

Die Festlegung, mit welcher Wahrscheinlichkeit innerhalb welcher Zeit diese Daten zur Verfügung stehen sollen, muß abhängig vom jeweiligen Anwendungsumfeld erfolgen.

FPT_ITA.1.1 Die TSF müssen die Verfügbarkeit von allen für sicherheitsrelevante Entscheidungen benötigten Daten, die für ein entferntes vertrauenswürdiges IT-Produkt bereitgestellt sind, innerhalb [Zuweisung: definierte Verfügbarkeitsmetrik] unter folgenden Bedingungen [Zuweisung: Bedingungen zum Sicherstellen der Verfügbarkeit] sicherstellen.

6.1.5.9 Vertraulichkeit von exportierten TSF-Daten (FPT_ITC)

Erläuterung: Diese Familie definiert die Schutzregeln gegen die nichtautorisierte Preisgabe von TSF-Daten während der Übertragung zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt. Diese Daten können zum Beispiel kritische TSF-Daten wie Paßworte, Schlüssel, Protokolldaten oder ausführbarer TSF-Code sein.

FPT_ITC.1 Vertraulichkeit bei Inter-TSF-Datenübertragung

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_ITC.1, die erfordert, daß die TSF sicherstellen, daß Daten, die zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt übertragen werden, während der Übertragung vor Preisgabe geschützt sind.

FPT_ITC.1.1 Die TSF müssen alle TSF-Daten, die von den TSF zu einem entfernten vertrauenswürdigen IT-Produkt übertragen werden, während der Übertragung vor nichtautorisierter Preisgabe schützen.

6.1.5.10 Integrität von exportierten TSF Daten (FPT_ITI)

Erläuterung: Diese Familie definiert die Schutzregeln gegen die nichtautorisierte Modifizierung von TSF-Daten während der Übertragung zwi-

schen TSF und einem entfernten vertrauenswürdigen IT-Produkt. Diese Daten können zum Beispiel kritische TSF-Daten wie Paßworte, Schlüssel, Protokolldaten oder ausführbarer TSF-Code sein.

FPT_ITI.1 Inter-TSF-Erkennung von Modifizierungen

Erläuterung: FPT_ITI.1 stellt die Fähigkeit bereit, Modifizierungen von TSF-Daten während der Übertragung zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt zu erkennen. Dies geschieht unter der Annahme, daß das entfernte vertrauenswürdige IT-Produkt mit dem benutzten Mechanismus vertraut ist.

FPT_ITI.1.1 Die TSF müssen die Fähigkeit bereitstellen, jede Modifizierung von TSF-Daten während der Übertragung zwischen den TSF und einem entfernten vertrauenswürdigen IT-Produkt innerhalb der folgenden Metrik: [Zuweisung: eine definierte Modifizierungsmetrik] zu erkennen.

Verfeinerung:
Die gewählte Metrik muß sicherstellen, daß die Integrität bezüglich der
- Veränderung sicherheitsrelevanter Systemdaten
- Löschung sicherheitsrelevanter Systemdaten
- Einfügung sicherheitsrelevanter Systemdaten
- Wiederholung sicherheitsrelevanter Systemdaten

auch während der Übertragung gewährleistet ist.

FPT_ITI.1.2 Die TSF müssen die Fähigkeit bereitstellen, die Integrität aller zwischen den TSF und einem entfernten, vertrauenswürdigen IT-Produkt übertragenen TSF-Daten zu verifizieren, und, falls Modifizierungen erkannt werden [Zuweisung: auszuführende Aktion] ausführen.

6.1.5.11 Erkennen von Wiedereinspielung (FPT_RPL)

Erläuterung: Diese Familie betrifft das Erkennen der Wiedereinspielung verschiedener Arten von Einheiten (zum Beispiel Nachrichten, Dienstanforderungen, Dienstereaktionen) und anschließenden Aktionen zur Korrektur. In dem Fall, wo eine Wiedereinspielung erkannt wird, wird diese hierdurch wirksam verhindert.

FPT_RPL.1 Erkennen von Wiedereinspielung

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_RPL.1 Erkennen von Wiedereinspielung, die von den TSF erfordert, daß diese in der Lage sein müssen, das Wiedereinspielen von identifizierten Einheiten zu erkennen.

FPT_RPL.1.1 Die TSF müssen eine Wiedereinspielung für die folgenden Einheiten erkennen:
- Authentisierungsdaten
- Tickets / Credentials.
- alle Daten einer geschützten Verbindung

FPT_RPL.1.2 Die TSF müssen bei Erkennung von Wiedereinspielung
- eine Zurückweisung der Aktion, die mit den wiedereingespielten Daten in Verbindung steht und
- eine Protokollierung des Vorfalls

durchführen.

6.1.5.12 Zeitstempel (FPT_STM)

Erläuterung: Diese Familie befaßt sich mit den Anforderungen an eine Funktion für verläßliche Zeitstempel innerhalb eines EVG.

FPT_STM.1 **Verläßliche Zeitstempel**

Erläuterung: Diese Familie besteht aus nur einer Komponente, FPT_STM.1, die erfordert, daß die TSF verläßliche Zeitstempel für TSF-Funktionen bereitstellen.

FPT_STM.1.1 Die TSF sollen einen verläßlichen Zeitstempel für den Eigengebrauch bereitstellen.

6.1.6 Kommunikation (FCO)

Erläuterung: Diese Klasse stellt zwei Familien bereit, die sich speziell mit der Sicherstellung der Identität der am Datenaustausch beteiligten Seiten befassen. Diese Familien beziehen sich auf die Sicherstellung der Identität eines Urhebers der übertragenen Informationen (Urheberschaftsbeweis) und die Sicherstellung der Identität des Empfängers der übertragenen Informationen (Empfangsbeweis). Diese Familien stellen sicher, daß ein Urheber nicht bestreiten kann, die Nachricht verschickt zu haben und daß auch der Empfänger den Empfang nicht leugnen kann.

6.1.6.1 Nichtabstreitbarkeit der Urheberschaft (FCO_NRO)

Erläuterung: Die Nichtabstreitbarkeit der Urheberschaft stellt sicher, daß der Urheber nicht erfolgreich bestreiten kann, eine Nachricht verschickt zu haben. Diese Familie erfordert, daß die TSF eine Methode bereitstellen, die sicherstellt, daß einem Subjekt, das während eines Datenaustausches Informationen empfängt, der Urheberschaftsnachweis dieser Informationen zur Verfügung gestellt wird. Dieser Nachweis kann dann entweder durch dieses oder andere Subjekte verifiziert werden.

FCO_NRO.1 **`Selektiver Urheberschaftsbeweis`**

Erläuterung: FCO_NRO.1 erfordert, daß die TSF den Subjekten die Fähigkeit zur Anforderung des Urheberschaftsnachweises von Informationen bereitstellen.

Die Möglichkeit der Überprüfung der Urheberschaftsnachweise ist zeitlich begrenzt auf die Gültigkeitsdauer des verwendeten Signaturverfahrens.

FCO_NRO.1.1 Die TSF müssen auf Anforderung des Urhebers für

- alle übertragenen Objekte, die über nicht vertrauenswürdige Pfade übermittelt werden
- alle übertragenen Objekte, für die aufgrund von rechtlichen Vorschriften ein Absendernachweis gegenüber einem neutralen Dritten erforderlich werden kann

Urheberschaftsnachweise generieren können.

FCO_NRO.1.2 Die TSF müssen die [Zuweisung: Liste der Attribute] des Informationsurhebers den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können.

FCO_NRO.1.3 Die TSF müssen

- dem Absender des Objektes
- dem Empfänger des Objektes
- einem befugten, neutralen Dritten

die Fähigkeit zum Verifizieren des Urheberschaftsnachweises von Informationen unter der Vorgabe von [Zuweisung: Begrenzungen des Urheberschaftsnachweises] bereitstellen.

6.1.6.2 Nichtabstreitbarkeit des Empfangs (FCO_NRR)

Erläuterung: Die Nichtabstreitbarkeit des Empfangs stellt sicher, daß der Empfänger der Informationen den Empfang der Informationen nicht erfolgreich bestreiten kann. Diese Familie erfordert, daß die TSF eine Methode bereitstellen, die sicherstellt, daß einem Subjekt, das während eines Datenaustausches Informationen übermittelt, einen Empfangsnachweis der Informationen zur Verfügung gestellt wird. Dieser Nachweis kann dann entweder durch dieses oder andere Subjekte verifiziert werden.

FCO_NRR.1 **Selektiver Empfangsbeweis**

Erläuterung: FCO_NRR.1 erfordert, daß die TSF den Subjekten die Fähigkeit zur Anforderung des Empfangsnachweises von Informationen bereitstellen.

FCO_NRR.1.1 Die TSF müssen auf Anforderung des Urhebers für

- empfangene elektronische Post
- alle empfangenen Objekte, für die aufgrund von rechtlichen Vorschriften ein Empfängernachweis erforderlich ist.

Empfangsnachweise generieren können.

FCO_NRR.1.2 Die TSF müssen die [Zuweisung: Liste der Attribute] des Informationsempfängers den [Zuweisung: Liste der Informationsfelder] der Informationen, auf die sich der Nachweis bezieht, zuordnen können.

FCO_NRR.1.3 Die TSF müssen die Fähigkeit zum Verifizieren des Empfangsnachweises von Informationen durch

- den Absender des Objektes
- den Empfänger des Objektes
- einen befugten, neutralen Dritten

unter Vorgabe von [Zuweisung: Begrenzungen des Empfangsnachweises] bereitstellen.

Verfeinerung:

Die Möglichkeit der Überprüfung ist zeitlich begrenzt auf die Gültigkeitsdauer des verwendeten Signaturverfahrens.

Das System soll dem Absender des Objektes erlauben, eine Empfangsbestätigung beim Versenden des Objektes anzufordern.

6.1.7 Vertrauenswürdiger Pfad/Kanal (FTP)

Erläuterung: Familien dieser Klasse stellen Anforderungen an einen vertrauenswürdigen Kommunikationspfad zwischen Benutzern und den TSF bereit, sowie an einen vertrauenswürdigen Kommunikationskanal zwischen den TSF und anderen vertrauenswürdigen IT-Produkten.

6.1.7.1 Vertrauenswürdiger Pfad (FTP_TRP)

Erläuterung: Diese Familie definiert die Anforderungen zum Einrichten und Verwalten einer vertrauenswürdigen Kommunikation zwischen den Benutzern und den TSF. Ein vertrauenswürdiger Pfad kann für jegliche sicherheitsrelevante Interaktion erforderlich sein. Ein Datenaustausch über einen vertrauenswürdigen Pfad kann durch den Benutzer während der Interaktion mit den TSF eingeleitet werden oder die TSF können die Kommunikation mit dem Benutzer über einen vertrauenswürdigen Pfad einrichten.

FTP_TRP.1 **Vertrauenswürdiger Pfad**

Erläuterung: FTP_TRP.1 erfordert, daß ein vertrauenswürdiger Pfad zwischen den TSF und einem Benutzer für eine von einem PP/ST-Verfasser definierte Menge von Ereignissen bereitgestellt wird. Der Benutzer und/oder die TSF können die Fähigkeit besitzen, den vertrauenswürdigen Pfad einzuleiten.

FTP_TRP.1.1 Die TSF müssen einen Kommunikationspfad zwischen sich und lokalen Benutzern bereitstellen, der logisch von den anderen Kommunikationspfaden getrennt ist und eine sichere Identifikation seiner Endpunkte sowie den Schutz der Kommunikationsdaten vor Modifizierung oder Preisgabe bereitstellt.

FTP_TRP.1.2 Die TSF müssen den TSF und den lokalen Benutzern erlauben, eine Kommunikation über den vertrauenswürdigen Pfad einzuleiten.

FTP_TRP.1.3 Die TSF müssen den Gebrauch des vertrauenswürdigen Pfads für

- die Erst-Benutzerauthentisierung,
- die Benutzung des Authentisierungsmechanismus (z.B. zur Re-Authentisierung),
- die Eingabe von sensitiven Informationen

erfordern.

6.1.7.2 Inter-TSF Vertrauenswürdiger Kanal (FTP_ITC)

Erläuterung: Diese Familie definiert Anforderungen zur Einrichtung eines vertrauenswürdigen Kanals zwischen den TSF und anderen vertrauenswürdigen IT-Produkten für die Ausführung von sicherheitskritischen Operationen.

FTP_ITC.1 **Inter-TSF Vertrauenswürdiger Kanal**

Erläuterung: FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal erfordert, daß die TSF einen vertrauenswürdigen Kommunikationskanal zwischen sich selbst und einem anderen vertrauenswürdigen IT-Produkt bereitstellen.

FTP_ITC.1.1 Die TSF müssen einen Kommunikationskanal zwischen sich und einem entfernten vertrauenswürdigen IT-Produkt bereitstellen, der logisch von

den anderen Kommunikationskanälen getrennt ist und eine sichere Identifikation seiner Endpunkte sowie den Schutz der Daten des Kanals vor Modifizierung oder Preisgabe bereitstellt.

FTP_ITC.1.2 Die TSF müssen den TSF und dem entfernten vertrauenswürdigen IT-Produkt erlauben, eine Kommunikation über den vertrauenswürdigen Kanal einzuleiten.

FTP_ITC.1.3 Die TSF müssen für

- die Übertragung sämtlicher sicherheitsrelevanter Systemdaten
- die Übertragung sämtlicher sicherheitsrelevanter Benutzerdaten

eine Kommunikation über den vertrauenswürdigen Kanal einleiten.

6.1.8 Kryptographische Unterstützung (FCS)

Erläuterung: Die TSF können kryptographische Funktionalität gebrauchen, um mehrere Sicherheitsziele auf hoher Ebene zu unterstützen. Diese umfassen u.a. Identifikation und Authentisierung, Nichtabstreitbarkeit, vertrauenswürdiger Pfad, vertrauenswürdiger Kanal und Datentrennung.

6.1.8.1 Kryptographischer Betrieb (FCS_COP)

Erläuterung: Damit eine kryptographische Operation korrekt funktioniert, muß diese Operation nach einem spezifizierten Algorithmus und mit einem kryptographischen Schlüssel einer spezifizierten Länge ausgeführt werden. Diese Familie sollte immer dann aufgenommen werden, wenn Anforderungen an die Durchführung von kryptographischen Operationen bestehen.

Typische kryptographische Operationen sind u.a. Datenverschlüsselung und/oder –entschlüsselung, Generierung und/oder Verifizierung von digitalen Unterschriften, kryptographische Prüfsummengenerierung für die Integrität und/oder Prüfsummenverifizierung, sichere Hash-Funktionen (Nachrichtenauswahl), Verschlüsselung und/oder Entschlüsselung des kryptographischen Schlüssels und die Vereinbarung von kryptographischen Schlüsseln.

FCS_COP.1 **Kryptographischer Betrieb**

Erläuterung: FCS_COP.1 erfordert, daß eine kryptographische Operation gemäß eines spezifizierten Algorithmus und mit einem kryptographischen Schlüssel von spezifizierter Länge ausgeführt wird. Der spezifizierte Algorithmus und die kryptographische Schlüssellänge können auf einer dafür bestimmten Norm basieren.

FCS_COP.1.1 Die TSF müssen alle kryptographischen Operationen gemäß eines vom ZKA zugelassenen kryptographischen Algorithmus und vom ZKA zugelassener kryptographischer Schlüssellängen durchführen.

6.1.8.2 Kryptographisches Schlüsselmanagement (FCS_CKM)

Erläuterung: Kryptographische Schlüssel müssen während ihres gesamten Lebenszyklus verwaltet werden. Diese Familie definiert Anforderungen an die folgenden Aktivitäten: Generierung kryptographischer Schlüssel, Verteilung kryptographischer Schlüssel, Zugriff auf kryptographischer Schlüssel und Zerstörung kryptographischer Schlüssel.

FCS_CKM.1 **Generierung des kryptographischen Schlüssels**

Erläuterung: FCS_CKM.1 erfordert die Erzeugung von kryptographischen Schlüsseln gemäß spezifizierter Algorithmen und Schlüssellängen, die auf einer dafür bestimmten Norm basieren können.

FCS_CKM.1.1 Die TSF müssen kryptographische Schlüssel gemäß eines spezifizierten Algorithmus zur Generierung des kryptographischen Schlüssels [Zuweisung: Algorithmus zur Generierung des kryptographischen Schlüssels] und spezifizierte kryptographische Schlüssellängen [Zuweisung: kryptographische Schlüssellängen], die den Standards des SIZ entsprechen, generieren.

FCS_CKM.1 Generierung des kryptographischen Schlüssels (Iteration)

FCS_CKM.1.1 Die TSF müssen kryptographische Schlüssel gemäß eines spezifizierten Algorithmus zur Generierung des kryptographischen Schlüssels [Zuweisung: Algorithmus zur Generierung des kryptographischen Schlüssels] und spezifizierte kryptographische Schlüssellängen [Zuweisung: kryptographische Schlüssellängen], die den Standards des ZKA für verbandsübergreifende Anwendungen entsprechen, generieren.

FCS_CKM.2 Verteilung des kryptographischen Schlüssels

Erläuterung: FCS_CKM.2 erfordert die Verteilung von kryptographischen Schlüsseln gemäß einer spezifizierten Verteilungsmethode, die auf einer dafür bestimmten Norm basieren kann.

FCS_CKM.2.1 Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Verteilung des kryptographischen Schlüssels [Zuweisung: Methode zur Verteilung des kryptographischen Schlüssels], die den folgenden [Zuweisung: Liste der Normen] entspricht, verteilen.

FCS_CKM.3 Zugriff auf den kryptographischen Schlüssel

Erläuterung: FCS_CKM.3 erfordert, daß der Zugriff auf kryptographische Schlüssel gemäß einer spezifizierten Zugriffsmethode durchgeführt wird, die auf einer dafür bestimmten Norm basieren kann.

FCS_CKM.3.1 Die TSF müssen den Zugriff auf kryptographische Schlüssel für

- die Sicherung von Schlüsseln (cryptographic key backup)
- die Archivierung von Schlüsseln (cryptographic key archival)
- die Hinterlegung von Schlüsseln (cryptographic key escrow)
- das Wiedererlangen von Schlüsseln (cryptographic key recovery)

gemäß einer vom ZKA zugelassenen Zugriffsmethode auf kryptographische Schlüssel durchführen.

FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

Erläuterung: FCS_CKM.4 erfordert die Zerstörung von kryptographischen Schlüsseln gemäß einer spezifizierten Zerstörungsmethode, die auf einer dafür bestimmten Norm basieren kann.

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

6.1.9 Sicherheitsprotokollierung (FAU)

Erläuterung: Zur Sicherheitsprotokollierung gehören das Erkennen, Aufzeichnen, Speichern und Analysieren von Informationen im Zusammenhang mit sicherheitsrelevanten (d.h. von der TSP kontrollierten) Aktivitäten. Die dabei entstehenden Protokollaufzeichnungen können untersucht werden, um zu ermitteln, welche sicherheitsrelevanten Aktivitäten ausgeführt wurden und wer (welcher Benutzer) dafür verantwortlich ist.

6.1.9.1 Generierung der Sicherheitsprotokolldaten (FAU_GEN)

Erläuterung: Diese Familie definiert Anforderungen an die Aufzeichnung des Auftretens sicherheitsrelevanter Ereignisse, die unter TSF-Kontrolle ausgeführt werden. Diese Familie identifiziert die Stufen der Protokollierung, zählt die Ereignistypen auf, die durch die TSF protokollierbar sein müssen, und gibt die Mindestmenge der protokollbezogenen Informationen an, die innerhalb der verschiedenen Arten von Protokollaufzeichnungen bereitgestellt werden müssen.

FAU_GEN.1 **Generierung der Protokolldaten**

Erläuterung: FAU_GEN.1 definiert die Stufe der protokollierbaren Ereignisse und spezifiziert eine Liste von Daten, die in jeder Aufzeichnung gespeichert werden müssen.

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

- Starten und Beenden der Protokollierungsfunktionen;
- Alle protokollierbaren Ereignisse für den Protokollierungsgrad „nicht angegeben“ und
- die nachfolgend festgelegten Ereignisse:

Funktion	Protokollierung
FIA	**Identifikation und Authentisierung**
FIA_UID.2	Einfach: Jeder Gebrauch des Benutzeridentifikationsmechanismus, einschließlich der bereitgestellten Benutzeridentität.
FIA_USB.1	Einfach: Erfolgreiche oder mißlungene Bindung von Benutzersicherheitsattributen an ein Subjekt [zum Beispiel Erfolg oder Mißerfolg bei Erzeugung eines Subjekts).
FIA_ATD.1	Keine Anforderungen.
FIA_UAU.2	Einfach: Jeder Gebrauch des Authentisierungsmechanismus.
FIA_UAU.4	Minimal: Versuche zur Wiederverwendung von Authentisierungsdaten

Funktion	Protokollierung
FIA_UAU.5	Einfach: Das Ergebnis jedes aktivierten Mechanismus zusammen mit der endgültigen Entscheidung.
FIA_UAU.6	Einfach: Alle Versuche einer Wiederauthentisierung.
FIA_UAU.7	Keine Anforderungen.
FIA_SOS.1	Einfach: Zurückweisung oder Annahme jeglicher getesteter Geheimnisse durch die TSF.
FIA_AFL.1	Minimal: Das Erreichen der Schwelle für die mißlungenen Authentisierungsversuche und die ausgeführten Aktionen (zum Beispiel Deaktivieren eines Terminals) und, wenn angemessen, die infolgedessen ausgeführte Wiederherstellung des normalen Zustands.
FTA	**EVG-Zugriff**
FTA_TSE.1	Einfach: Alle Versuche zur Einrichtung einer Benutzersitzung. Detailliert: Erfassen der Werte der ausgewählten Zugangsparameter (zum Beispiel Ort und Zeit des Zugangs).
FTA_LSA.1	Einfach: Alle Versuche zur Auswahl von Sitzungs-Sicherheitsattributen. Detailliert: Erfassen der Werte jedes Sitzungs-Sicherheitsattributs.
FTA_SSL.1, FTA_SSL.2	Minimal: Sperren einer interaktiven Sitzung durch den Sitzungssperr-Mechanismus. Einfach: Alle Versuche, eine interaktive Sitzung zu entsperren.
FTA_MCS.1	Minimal: Zurückweisung einer neuen Sitzung aufgrund der Begrenzung von mehreren gleichzeitigen Sitzungen.
FTA_TAH.1	Keine Anforderungen.
FDP	**Schutz der Benutzerdaten**
FDP_ACC.1 (DAC), FDP_ACC.1 (RBAC)	Keine Anforderungen.
FDP_ACF.1 (DAC), FDP_ACF.1 (RBAC)	Minimal: Erfolgreiche Anforderungen zur Durchführung einer Operation mit einem durch die SFP abgedeckten Objekt. Einfach: Alle Anforderungen zur Durchführung einer Operation mit einem durch SFP abgedeckten Ob-

Funktion	Protokollierung
	jekt.
FDP_SDI.2	Einfach: Alle Versuche der Integritätsüberprüfung von Benutzerdaten, einschließlich Anzeige der Ergebnisse der tatsächlich erfolgten Überprüfungen.
FDP_UCT.1	Minimal: Die Identität aller Benutzer oder Subjekte, die den Datenaustauschmechanismus benutzen. Einfach: Die Identität aller nichtautorisierten Benutzer, die versuchen, die Datenaustauschmechanismen zu benutzen. Einfach: Verweise auf Namen oder andere ordnende Informationen, die für die Identifikation übertragener bzw. empfangener Benutzerdaten nützlich sind. Dies können z.B. die mit den Informationen verknüpften Sicherheitsattribute sein.
FDP_UIT.1	Minimal: Die Identität aller Benutzer oder Subjekte, die den Datenaustauschmechanismus nutzen. Einfach: Die Identität aller Benutzer oder Subjekte, die versuchen, den Datenaustauschmechanismus zu nutzen, dazu jedoch nicht autorisiert sind. Einfach: Verweise auf Namen oder andere ordnende Informationen, die für die Identifikation übertragener bzw. empfangener Benutzerdaten nützlich sind. Dies können z.B. die mit den Benutzerdaten verknüpften Sicherheitsattribute sein.
FDP_RIP.2	Keine Anforderungen.
FPT	**Schutz der EVG-Sicherheitsfunktionen**
FPT_PHP.3	Keine Anforderungen.
FPT_RVM.1	Keine Anforderungen.
FPT_SEP.2	Keine Anforderungen.
FPT_AMT.1	Einfach: Ausführung der Tests der zugrundeliegenden Maschine und die Ergebnisse dieser Tests.
FPT_TST.1	Einfach: Ausführung des TSF-Selbsttests und die Ergebnisse der Tests.
FPT_FLS.1	Einfach: TSF-Fehler.
FPT_RCV.1	Minimal: Die Tatsache, daß ein Fehler oder eine Diensteunterbrechung aufgetreten ist. Minimal: Wiederaufnahme des regulären Betriebs. Einfach: Art des Fehlers oder der Diensteunterbrechung.

Funktion	Protokollierung
FPT_ITA.1	Minimal: Die Abwesenheit von TSF-Daten, wenn diese von einem EVG benötigt werden.
FPT_ITC.1	Keine Anforderungen.
FPT_ITI.1	Minimal: Erkennung von Modifizierungen übertragener TSF-Daten. Einfach: Aktion bei Erkennung von Modifizierungen übertragener TSF-Daten.
FPT_RPL.1	Einfach: Erkannte Wiedereinspielungsangriffe.
FPT_STM.1	Minimal: Änderungen der Zeit.
FCO	**Kommunikation**
FCO_NRO.1	Minimal: Die Identität des die Generierung des Urheberschaftsnachweises fordernden Benutzers. Minimal: Aufruf des Nichtabstreitbarkeits-Dienstes.
FCO_NRR.1	Minimal: Die Identität des die Generierung des Empfangsnachweises fordernden Benutzers. Minimal: Aufruf des Nichtabstreitbarkeits-Dienstes.
FTP	**Vertrauenswürdiger Pfad/Kanal**
FTP_TRP.1	Minimal: Fehler der Funktionen des vertrauenswürdigen Pfads. Minimal: Identifikation des Benutzers, falls vorhanden, der mit allen Fehlern des vertrauenswürdigen Pfads verknüpft ist. Einfach: Jeder versuchte Gebrauch der Funktionen des vertrauenswürdigen Pfads. Einfach: Identifikation des Benutzers, falls vorhanden, der mit allen Aufrufen des vertrauenswürdigen Kanals verknüpft ist.
FTP_ITC.1	Minimal: Fehler der Funktionen des vertrauenswürdigen Kanals. Minimal: Identifikation des Initiators und des Ziels der Funktionen des vertrauenswürdigen Kanals, die fehlschlugen. Einfach: Jeder versuchte Gebrauch der Funktionen des vertrauenswürdigen Kanals. Einfach: Identifikation des Initiators und des Ziels aller Funktionen des vertrauenswürdigen Kanals.

Funktion	Protokollierung
FCS	**Kryptographische Unterstützung**
FCS_COP.1	Minimal: Erfolg, Mißerfolg und Art der kryptographischen Operation. Einfach: Jede geeignete kryptographische Betriebsart, Subjektattribute und Objektattribute.
FCS_CKM.1 - bis FCS_CKM.4	Minimal: Erfolg oder Mißerfolg der Aktivität. Einfach: Objektattribut(e) und Objektwert(e) mit Ausnahme irgendwelcher sensitiven Informationen (zum Beispiel geheime oder private Schlüssel).
FAU	**Sicherheitsprotokollierung**
FAU_GEN.1	Keine Anforderungen.
FAU_GEN.2	Keine Anforderungen.
FAU_SEL.1	Minimal: Alle Modifizierungen der Protokollierungs-Konfiguration, die während des Betriebs der Protokolldatenerfassungs-Funktionen auftreten.
FAU_SAA.1	Minimal: Aktivieren oder Deaktivieren irgendeines Analysemechanismusses. Minimal: Ausführen automatischer Reaktionen durch das Werkzeug.
FAU_ARP.1	Minimal: Ausgeführte Aktionen wegen drohender Sicherheitsverletzungen.
FAU_STG.2	Keine Anforderungen.
FAU_STG.4	Einfach: Aktionen, die wegen eines Protokollspeicherfehlers ausgeführt werden.
FAU_SAR.1	Keine Anforderungen.
FAU_SAR.2	Einfach: Mißlungene Versuche des Lesens von Informationen aus Protokollaufzeichnungen.
FAU_SAR.3	Keine Anforderungen.
FMT	**Sicherheitsmanagement**
FMT_MOF.1	Einfach: Alle Modifizierungen im Verhalten der Funktionen in den TSF.
FMT_MSA.1	Einfach: Alle Modifizierungen von Werten der Sicherheitsattribute.
FMT_MSA.2	Minimal: Alle vorgeschlagenen und zurückgewiesenen Werte für ein Sicherheitsattribut. Detailliert: Alle vorgeschlagenen und akzeptierten sicheren Werte für ein Sicherheitsattribut.
FMT_MSA.3	Einfach: Modifizierungen der vorgegebenen Stan-

Funktion	Protokollierung
	dardeinstellung von freizügigen oder einschränkenden Regeln.
FMT_MTD.1	Einfach: Alle Modifizierungen der Werte von TSF-Daten.
FMT_MTD.2	Einfach: Alle Modifizierungen der Begrenzungen für TSF-Daten.
FMT_REV.1	Einfach: Mißlungener Widerruf von Sicherheitsattributen
FMT_SAE.1	Einfach: Spezifikation der Verfallzeit für ein Attribut. Einfach: Aktion, die wegen Attributverfalls auszuführen ist.
FMT_SMR.1	Minimal: Modifizierungen der Gruppe von Benutzern, die Teil einer Rolle sind.
FMT_SMR.2	Minimal: Modifizierungen der Gruppe von Benutzern, die Teil einer Rolle sind Minimal: Mißlungene Versuche des Gebrauchs einer Rolle aufgrund bestimmter Bedingungen der Rolle
FMT_SMR.3	Minimal: Explizite Anforderung zur Annahme einer Rolle

Tabelle 2: Zu protokollierende Ereignisse

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

- Datum und Uhrzeit des Ereignisses,
- Art des Ereignisses,
- Identität des Subjekts und
- das Ergebnis (Erfolg oder Mißerfolg) des Ereignisses

und basierend auf den Definitionen eines in PP/ST eingebundenen protokollierbaren Ereignisses für jede Art von Protokollierungsereignissen die Informationen, die erforderlich sind, um die in FAU_GEN.1.1 beschriebenen Protokollinformationen zu erzeugen.

FAU_GEN.2 **Verknüpfung der Benutzeridentität**

Erläuterung: Bei FAU_GEN.2 müssen die TSF protokollierbare Ereignisse mit individuellen Benutzeridentitäten verknüpfen.

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.

6.1.9.2 Ereignisauswahl für die Sicherheitsprotokollierung (FAU_SEL)

Erläuterung: Diese Familie definiert Anforderungen zur Auswahl der Ereignisse, die während des EVG-Betriebs zu protokollieren sind. Sie definiert Anforderungen zum Aufnehmen oder Ausschließen von Ereignissen in die oder aus der Menge der protokollierbaren Ereignisse.

FAU_SEL.1 **Auswahl der Ereignisse für die Sicherheitsprotokollierung**

Erläuterung: FAU_SEL.1 erfordert die Fähigkeit, auf Grundlage von Attributen Ereignisse in die Menge der protokollierten Ereignisse aufzunehmen oder auszuschließen.

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:

- Objektidentität,
- Benutzeridentität,
- Subjektidentität,
- Hostrechneridentität
- Ereignisart

6.1.9.3 Analyse der Sicherheitsprotokollierung (FAU_SAA)

Erläuterung: Diese Familie definiert Anforderungen an automatische Mittel zur Analyse von Systemaktivitäten und Protokolldaten auf mögliche oder tatsächliche Sicherheitsverletzungen. Diese Analyse kann zur Unterstützung bei der Eindringerkennung oder der automatischen Reaktion auf drohende Sicherheitsverletzungen dienen.

FAU_SAA.1 **Analyse von möglichen Verletzungen**

Erläuterung: In FAU_SAA.1 wird eine einfache Schwellenerkennung auf Basis einer festgelegten Menge von Regeln gefordert.

FAU_SAA.1.1 Die TSF müssen in der Lage sein, beim Überwachen der protokollierten Ereignisse eine Menge von Regeln anzuwenden und auf Grundlage dieser Regeln eine potentielle Verletzung der TSP anzuzeigen.

FAU_SAA.1.2 Die TSF müssen zur Überwachung von protokollierten Ereignissen die folgenden Regeln durchsetzen:

- Eine Häufung oder Kombination von
  - abgewiesenen Anmeldeversuchen innerhalb eines bestimmten Zeitraumes
  - abgewiesenen Anmeldeversuchen einer einzelnen Benutzerkennung
  - abgewiesenen Anmeldeversuchen von einem einzelnen Zugangspunkt aus
  - abgewiesenen Zugriffen auf Objekte innerhalb eines bestimmten Zeitraums
  - abgewiesenen Zugriffen auf ein einzelnes Objekt
  - abgewiesenen Zugriffen auf Objekte durch eine einzelne Benutzerkennung
  - abgewiesenen Zugriffen auf Objekte von einem einzelnen Zugangspunkt aus,

die bekannterweise eine potentielle Sicherheitsverletzung anzeigen, muß erkannt werden.

6.1.9.4 Automatische Reaktion der Sicherheitsprotokollierung (FAU_ARP)

Erläuterung: Diese Familie definiert die auszuführende Reaktion für den Fall, daß auf potentielle Sicherheitsverletzungen hindeutende Ereignisse entdeckt werden.

FAU_ARP.1 **`Sicherheitsalarme`**

Erläuterung: Bei FAU_ARP.1 müssen die TSF reagieren, falls eine potentielle Sicherheitsverletzung entdeckt wurde.

FAU_ARP.1.1 Die TSF müssen

- die Alarmierung eines verantwortlichen Systemadministrators
- eine Vereitelung der Sicherheitsverletzung durch eine der folgenden Aktionen
  - Herunterfahren des Systems;
  - Sperrung des Zugangspunktes oder Dienstes, über den die potentielle Sicherheitsverletzung erfolgt;
  - Sperrung der Benutzerkennung, von der aus die potentielle Sicherheitsverletzung erfolgt;
  - Entfernen des Subjektes, von dem aus die potentielle Sicherheitsverletzung erfolgt;
  - Entfernen aller Subjekte mit der Benutzerkennung, von der aus die potentielle Sicherheitsverletzung erfolgt;
  - Starten eines Programmes;

bei Erkennung einer potentiellen Sicherheitsverletzung ausführen.

6.1.9.5 Ereignisspeicherung der Sicherheitsprotokollierung (FAU_STG)

Erläuterung: Diese Familie definiert die Anforderungen an die TSF zur Erstellung und Erhaltung sicherer Protokolle durch die TSF.

FAU_STG.2 **`Garantie der Verfügbarkeit der Protokolldaten`**

Erläuterung: FAU_STG.2 spezifiziert die Garantien, die die TSF bei Auftreten einer unerwünschten Bedingung für die Protokolldaten erhalten.

FAU_STG.2.1 Die TSF müssen die gespeicherten Protokollaufzeichnungen gegen nichtautorisiertes Löschen schützen.

FAU_STG.2.2 Die TSF müssen Modifizierungen der Protokollaufzeichnungen erkennen und verhindern können.

FAU_STG.2.3 Die TSF müssen sicherstellen, daß bei Auftreten einer der folgenden Bedingungen

- Protokollspeicher erschöpft
- Fehler
- Angriff

bis auf eine festgelegte Anzahl von Einträgen, deren Verlust toleriert wird, alle Protokollaufzeichnungen erhalten werden.

FAU_STG.4 **Schutz vor Protokolldaten-Verlust**

Erläuterung: FAU_STG.4 Schutz vor Protokolldaten-Verlust spezifiziert Aktionen für den Fall, daß das Protokoll voll ist.

FAU_STG.4.1 Die TSF müssen, wenn das Protokoll voll ist,

- protokollierbare Ereignisse ignorieren oder
- protokollierbare Ereignisse verhindern, ausgenommen solche, die von einem autorisierten Benutzer mit besonderen Rechten herbeigeführt werden

und einen befugten Systemadministrator über den Überlauf des Protokolls informieren.

Verfeinerung:

Dem befugten Systemadministrator soll es möglich sein festzulegen, ob das Auftreten zu protokollierender Ereignisse ignoriert oder verhindert werden soll (mit Ausnahme der Aktionen des befugten Systemadministrators selbst).

6.1.9.6 Durchsicht der Sicherheitsprotokollierung (FAU_SAR)

Erläuterung: Diese Familie definiert die Anforderungen an Protokollierungswerkzeuge, die den autorisierten Benutzern zur Durchsicht der Protokolldaten zur Verfügung stehen sollen.

FAU_SAR.1 **Durchsicht der Protokollierung**

Erläuterung: FAU_SAR.1 stellt die Fähigkeit bereit, Informationen aus Protokollaufzeichnungen zu lesen.

FAU_SAR.1.1 Die TSF müssen für die befugten Systemadministratoren die Fähigkeit bereitstellen, sämtliche Informationen über protokollierte Ereignisse aus den Protokollaufzeichungen 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.

FAU_SAR.2 **Eingeschränkte Durchsicht der Protokollierung**

Erläuterung: FAU_SAR.2 erfordert, daß keine anderen Benutzer als diejenigen, die in FAU_SAR.1 identifiziert sind, die Informationen lesen können.

FAU_SAR.2.1 Die TSF müssen allen Benutzern Zugriff zum Lesen der Protokollaufzeichnungen verbieten, mit Ausnahme derjenigen Benutzer, denen der Lesezugriff explizit gewährt wurde.

FAU_SAR.3 **Auswählbare Durchsicht der Protokollierung**

Erläuterung: FAU_SAR.3 erfordert Werkzeuge zur Durchsicht der Protokollierung, mit denen Protokollierungsdaten auf Grundlage von Kriterien durchgesehen werden können.

FAU_SAR.3.1 Die TSF müssen die Fähigkeit der Ausführung von Suchen und Sortieren von Protokolldaten auf Grundlage von

- Benutzerkennungen
- Kennungen eines Subjektes

- Kennungen von Objekten (z.B. Pfadname)
- Zeiträumen
- Ereignissen, die eine Protokollierung ausgelöst haben

bereitstellen.

Verfeinerung:

Die Kriterien sollen für die Suche und die Sortierung unabhängig voneinander gewählt werden können.

Es soll möglich sein, verschiedene Kriterien durch logische Operatoren (UND, ODER) zu verknüpfen.

6.1.10 Sicherheitsmanagement (FMT)

Erläuterung: Diese Klasse ist zur Spezifikation des Managements vielfältiger Aspekte der TSF vorgesehen: Sicherheitsattribute, TSF-Daten und TSF-Funktionen.

6.1.10.1 Management der TSF-Funktionen (FMT_MOF)

Erläuterung: Diese Familie erlaubt autorisierten Benutzern die Kontrolle über das Management von Funktionen in den TSF. Beispiele für Funktionen in den TSF sind die Protokollierungsfunktion und die mehrfache Authentisierung.

FMT_MOF.1 **Management des Verhaltens der Sicherheitsfunktionen**

Erläuterung: FMT_MOF.1 erlaubt es autorisierten Benutzern (Rollen), das Verhalten von Funktionen in den TSF zu verwalten, die Regeln benutzen oder spezifizierte Bedingungen besitzen, die verwaltet werden können.

FMT_MOF.1.1 Die TSF müssen die Fähigkeit zum

- Feststellen des Verhaltens
- Deaktivieren
- Aktivieren
- Modifizieren des Verhaltens

aller konfigurierbaren Sicherheitsfunktionen auf die autorisierten identifizierten Rollen beschränken.

Die konfigurierbaren Sicherheitsfunktionen umfassen folgende Funktionen

Funktion	Managementaktivitäten
FIA	**Identifikation und Authentisierung**
FIA_UID.2	Management der Benutzeridentitäten.
FIA_USB.1	Autorisierte Systemverwalter können Standardvorgaben für Subjektsicherheitsattribute definieren.
FIA_ATD.1	Autorisierte Systemverwalter können in der Lage sein, zusätzliche Sicherheitsattribute zu definieren.

Funktion	Managementaktivitäten
FIA_UAU.2	Management der Authentisierungsdaten durch einen Systemverwalter.
FIA_UAU.4	Keine Managementaktivitäten.
FIA_UAU.5	Management von Authentisierungsmechanismen.
FIA_UAU.6	Management der Funktionen zur Wiederauthentisierung.
FIA_UAU.7	Keine Managementaktivitäten.
FIA_SOS.1	Management der zur Verifizierung der Geheimnisse benutzten Metrik.
FIA_AFL.1	Management der Schwelle für mißlungene Authentisierungsversuche. Management der im Falle eines Authentisierungsfehlers durchzuführenden Aktionen.
FTA	**EVG-Zugriff**
FTA_TSE.1	Management der Sitzungseinrichtungsbedingungen durch den autorisierten Systemverwalter.
FTA_LSA.1	Management des Anwendungsbereichs der Sitzungs-Sicherheitsattribute durch einen Systemverwalter.
FTA_SSL.1	Spezifikation der Dauer der Benutzerinaktivität, nach der ein einzelner Benutzer gesperrt wird. Management von Ereignissen, die vor dem Entsperren der Sitzung eintreten sollen. Spezifikation der Standardvorgabe für die Dauer der Benutzerinaktivität, nach der die Sperrung erfolgt.
FTA_SSL.2	Management von Ereignissen, die vor dem Entsperren der Sitzung eintreten sollen.
FTA_MCS.1	Management der maximal zulässigen Anzahl von gleichzeitigen Benutzersitzungen durch einen Systemverwalter.
FTA_TAH.1	Keine Managementaktivitäten.
FDP	**Schutz der Benutzerdaten**
FDP_ACC.1 (RBAC)	Keine Managementaktivitäten.
FDP_ACF.1 (RBAC)	Verwalten der Attribute, die für explizite Entscheidungen auf der Grundlage von Zugriff oder Zugriffsverweigerung verwendet werden. Dies beinhaltet die Verwaltung der Zugriffskontrollisten von Objekten und die Verwaltung der Rollenhierarchie, die die Vererbung von Rollen bestimmt.
FDP_ACC.1 (DAC)	Keine Managementaktivitäten.

Funktion	Managementaktivitäten
FDP_ACF.1 (DAC)	Verwalten der Attribute, die für explizite Entscheidungen auf der Grundlage von Zugriff oder Zugriffsverweigerung verwendet werden.
FDP_SDI.1	Keine Managementaktivitäten.
FDP_UCT.1	Keine Managementaktivitäten.
FDP_UIT.1	Keine Managementaktivitäten.
FDP_RIP.2	Keine Managementaktivitäten.
FPT	**Schutz der EVG-Sicherheitsfunktionen**
FPT_PHP.3	Management der automatischen Reaktionen auf materielle Manipulationen
FPT_RVM.1	Keine Managementaktivitäten.
FPT_SEP.2	Keine Managementaktivitäten.
FPT_AMT.1	Management der Bedingungen, unter denen Tests der abstrakten Maschine erfolgen, beispielsweise bei Erstanlauf, in regelmäßigen Abständen bzw. bei spezifizierten Bedingungen. Zeitintervall-Management, falls angemessen.
FPT_TST.1	Management der Bedingungen, unter denen ein TSF-Selbsttest erfolgt, zum Beispiel während des Erstanlaufs, in regelmäßigen Abständen, oder unter spezifizierten Bedingungen. Zeitintervall-Management, falls angemessen.
FPT_FLS.1	Keine Managementaktivitäten.
FPT_RCV.1	Management der Zugriffsberechtigten auf die Wiederherstellfähigkeit im Erhaltungsmodus.
FPT_ITA.1	Management der Artenliste von TSF-Daten, die für ein entferntes vertrauenswürdiges IT-Produkt verfügbar sein müssen.
FPT_ITC.1	Keine Managementaktivitäten.
FPT_ITI.1	Keine Managementaktivitäten.
FPT_RPL.1	Management der Liste von identifizierten Einheiten, für die eine Wiedereinspielung erkannt werden muß; Management der Liste von Aktionen, die im Falle von Wiedereinspielung auszuführen sind.
FPT_STM.1	Zeitmanagement
FCO	**Kommunikation**
FCO_NRO.1	Management der Änderungen von Informationsarten, Feldern, Urheberattributen und Empfangsnachweisen.

Funktion	Managementaktivitäten
FCO_NRR.1	Management der Änderungen von Informationsarten, Feldern, Urheberattributen und Drittempfängern von Nachweisen.
FTP	**Vertrauenswürdiger Pfad/Kanal**
FTP_TRP.1	Konfigurieren der Aktionen, die einen vertrauenswürdigen Pfad erfordern, falls unterstützt.
FTP_ITC.1	Konfiguration der Aktionen, die einen vertrauenswürdigen Kanal erfordern, falls unterstützt.
FCS	**Kryptographische Unterstützung**
FCS_COP.1	Keine Managementaktivitäten.
FCS_CKM.1 bis FCS_CKM.4	Management von Änderungen an kryptographischen Schlüsseln. Beispiele für Schlüsselattribute sind u.a. Benutzer, Art des Schlüssels (zum Beispiel öffentlich, privat, geheim), Gültigkeitsdauer und Verwendung (zum Beispiel digitale Unterschrift, Verschlüsselung des Schlüssels, Schlüsselvereinbarung, Datenverschlüsselung).
FAU	**Sicherheitsprotokollierung**
FAU_GEN.1	Keine Managementaktivitäten.
FAU_GEN.2	Keine Managementaktivitäten.
FAU_SEL.1	Erhaltung der Rechte, die Protokollierungsereignisse anzusehen/zu modifizieren.
FAU_SAA.1	Erhaltung (Entfernen, Modifizieren, Hinzufügen) der Systemereignis-Teilmenge. Erhaltung (Löschen, Modifizieren, Hinzufügen) der Menge von Systemereignisfolgen.
FAU_ARP.1	Das Management von Aktionen (Hinzufügen, Entfernen oder Modifizierung).
FAU_SAR.1	Erhaltung (Löschen, Modifizieren, Hinzufügen) der Benutzergruppe mit Zugriffsberechtigung zum Lesen der Protokollaufzeichnungen.
FAU_SAR.2	Keine Managementaktivitäten.
FAU_SAR.3	Keine Managementaktivitäten.
FAU_STG.2	Erhaltung der Parameter, die die Protokollspeicherfähigkeit kontrollieren
FAU_STG.4	Erhaltung (Löschen, Modifizieren, Hinzufügen) von Aktionen, die im Falle von Protokollspeicherfehlern auszuführen sind.
FMT	**Sicherheitsmanagement**
FMT_MOF.1	Verwalten der Gruppe von Rollen, die mit den Funktionen

Funktion	Managementaktivitäten
	in den TSF interagieren kann.
FMT_MSA.1	Verwalten der Gruppe von Rollen, die mit den Sicherheitsfunktionen interagieren kann.
FMT_MSA.2	Keine Managementaktivitäten.
FMT_MSA.3	Verwalten der Gruppe von Rollen, die Anfangswerte spezifizieren kann. Verwalten der freizügigen und einschränkenden Einstellung der vorgegebenen Standardwerte für eine gegebene SFP für Zugriffskontrolle.
FMT_MTD.1	Verwalten der Gruppe von Rollen, die mit den TSF-Daten interagieren kann.
FMT_MTD.2	Verwalten der Gruppe von Rollen, die mit den Begrenzungen der TSF-Daten interagieren kann.
FMT_REV.1	Verwalten der Rollengruppe, die einen Widerruf von Sicherheitsattributen aktivieren kann. Verwalten der Listen der Benutzer, Subjekte, Objekte und anderen Betriebsmittel, bei denen Widerruf möglich ist. Verwalten der Widerrufregeln.
FMT_SAE.1	Verwalten der Liste der Sicherheitsattribute, für die der Verfall unterstützt sein muß;
FMT_SMR.1	Verwalten der Gruppe von Benutzern, die Teil einer Rolle sind.
FMT_SMR.2	Verwalten der Gruppe von Benutzern, die Teil einer Rolle sind; Verwalten der Bedingungen, die die Rollen erfüllen müssen.
FMT_SMR.3	Keine Managementaktivitäten

Tabelle 3: Managementaktivitäten der konfigurierbaren Sicherheitsfunktionen

6.1.10.2 Management der Sicherheitsattribute (FMT_MSA)

Erläuterung: Diese Familie erlaubt autorisierten Benutzern, das Management der Sicherheitsattribute zu kontrollieren. Dieses Management kann Berechtigungen zur Ansicht und Modifizierung von Sicherheitsattributen einschließen.

FMT_MSA.1 Management der Sicherheitsattribute

Erläuterung: FMT_MSA.1 erlaubt autorisierten Benutzern (Rollen) die Verwaltung der spezifizierten Sicherheitsattribute.

FMT_MSA.1.1 Die TSF müssen die benutzerbestimmte Zugriffskontrolle (DAC) zur Beschränkung der Fähigkeit zum Modifizieren der Sicherheitsattribute auf die gemäß nachfolgender Tabelle identifizierten Rollen durchsetzen.

Sicherheitsattribute	Aktion	erlaubte Rollen
Initialgeheimis bei Verwendung eines benutzeränderbaren Authentisierungsgeheimnisses	Setzen	• Sicherheitsadministrator für die Benutzerverwaltung
benutzeränderbares Authentisierungsgeheimnis	Modifizieren	• Sicherheitsadministrator für die Benutzerverwaltung • der jeweilige Benutzer
Sicherheitsattribute für jeden unterstützten Authentisierungsmechanismus (z.B. Anzahl der PW-Änderungen pro Tag)	Modifizieren der Standardvorgabe, Modifikation, Löschen	• Sicherheits-Systemtechniker • Kryptobeauftragter
Benutzerkennung, Liste der Rollen eines Benutzers, Liste der Gruppen eines Benutzers	Anlegen Modifizieren Löschen	• Sicherheitsadministrator für die Benutzerverwaltung
Rollen	Anlegen Modifizieren Löschen Zuordnen (zu anderen Rollen)	• Sicherheitsadministrator für die Rollenverwaltung
Systemzeit	Modifizieren	• Systemadministrator
Sitzungsparameter (z.B. erlaubte Login-Zeiten und –Zugangspunkte, Dauer Benutzerinaktivität) FTA_TSE.1, FTA_LSA.1, FTA_SSL.1)	Anlegen Modifizieren Löschen Zuordnen	• Sicherheits-Systemtechniker
Sitzungsparameter (z.B. erlaubte Login-Zeiten und -Zugangspunkte, Dauer Benutzerinaktivität) FTA_TSE.1, FTA_LSA.1, FTA_SSL.1)	Anzeigen	• jeder Benutzer
Sicherheitsrelevante Attribute von Objekten, die einer Zugriffskontrolle unterliegen (Besitzer/Ersteller des Objektes, Zugriffskontrolliste für DAC-kontrollierte Objekte, Liste der Rollen und der erlaubten Zugriffsmodi für RBAC-	Anlegen Modifizieren Löschen Zuordnen	• Sicherheits-Systemtechniker, • Ersteller/Besitzer des Objektes

Sicherheitsattribute	Aktion	erlaubte Rollen
kontrollierte Objekte, falls das Objekt der RBAC-Zugriffskontrolle unterliegt)		
alle anderen Attribute	Modifizieren der Standardvorgabe	• Systemadministrator

Tabelle 4: Modifikation von Sicherheitsattributen

FMT_MSA.2 **Sichere Sicherheitsattribute**

Erläuterung: FMT_MSA.2 stellt sicher, daß den Sicherheitsattributen zugewiesene Werte in Bezug auf den sicheren Zustand gültig sind.

FMT_MSA.2.1 Die TSF müssen sicherstellen, daß nur sichere Werte für Sicherheitsattribute akzeptiert werden.

FMT_MSA.3 **Initialisierung statischer Attribute**

Erläuterung: FMT_MSA.3 stellt sicher, daß vorgegebene Standardwerte von Sicherheitsattributen je nach Angemessenheit entweder von freizügiger oder einschränkender Natur sind.

FMT_MSA.3.1 Die TSF müssen die benutzerbestimmte Zugriffskontrolle (DAC) zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

Verfeinerung:

Folgende Vorgabewerte sollen für bestimmte Sicherheitsattribute gelten, falls dieses Attribut im System definiert ist:

Sicherheitsattribut	Vorgabewert
Gültigkeit einer Benutzerkennung	1 Jahr
Gültigkeit eines benutzerwählbaren Paßwortes	30 Tage
Dauer, die eine Kennung unbenutzt bleiben darf	60 Tage
Anzahl der aufeinanderfolgenden Fehlversuche bei der Authentisierung	3 Fehlversuche
Zeitspanne der Benutzerinaktivität bis zum vom System eingeleiteten Sperren einer interaktiven Sitzung.	10 Minuten
Anzahl der gleichzeitigen interaktiven Sitzungen pro Benutzer	1 Sitzung

Tabelle 5: Vorgabewerte für Sicherheitsattribute

FMT_MSA.3.2 Die TSF müssen dem Ersteller eines Objektes gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

6.1.10.3 Management der TSF Daten (FMT_MTD)

Erläuterung: Diese Familie erlaubt autorisierten Benutzern (Rollen) die Kontrolle über das Management der TSF-Daten. Beispiele für TSF-Daten sind Protokollinformationen, Uhr, Systemkonfiguration und andere Parameter der TSF-Konfiguration.

FMT_MTD.1 **Management der TSF-Daten**

Erläuterung: FMT_MTD.1 erlaubt autorisierten Benutzern, TSF-Daten zu verwalten.

FMT_MTD.1.1 Die TSF müssen die Fähigkeit zum

- Standardvorgaben ändern,
- Abfragen,
- Modifizieren,
- Löschen,
- Zurücksetzen,
- [Zuweisung: andere Operationen] (z.B. Erzeugen)

folgender TSF-Daten auf folgende Rollen beschränken:

TSF-Daten	Rollen
Protokollierungsdaten des Audit-Trails	Auditor
System-Konfigurationsdateien	Sicherheits-Systemtechniker
Audit-Konfigurationsdateien (z.B. Liste der zu protokollierenden Ereignisse)	Auditor
Benutzerkonten-Datenbanken (z.B. Authentisierungsdaten)	Sicherheitsadministrator für die Benutzerverwaltung
Systemuhr	Systemadministrator
[Zuweisung: Liste weiterer TSF-Daten]	[Zuweisung: autorisierten identifizierten Rollen]

Tabelle 6: Modifikation von TSF-Daten

FMT_MTD.2 **Management der Begrenzungen für TSF-Daten**

Erläuterung: FMT_MTD.2 spezifiziert die Aktion, die bei Erreichen oder Überschreiten der Begrenzungen für TSF-Daten auszuführen ist.

FMT_MTD.2.1 Die TSF müssen die Spezifikation der Begrenzungen für

- die Größe des Audit-Trails

auf die Rolle des Auditors beschränken.

FMT_MTD.2.2 Die TSF müssen die folgenden Aktionen ausführen, wenn TSF-Daten die angezeigten Begrenzungen erreicht haben oder diese überschreiten:

- Das System soll einen Alarm auslösen und einem verantwortlichen Systemadministrator zustellen, wenn die Größe des Audit-Trails eine vorbestimmte Grenze überschreitet.

6.1.10.4 Widerruf (FMT_REV)

Erläuterung: Die Anforderungen dieser Familie betreffen den Widerruf von Sicherheitsattributen in verteilten Systemen, wo die Änderung eines Sicherheitsattributes nicht unter allen Umständen sofort von den Sicherheitsfunktionen wahrgenommen wird.

FMT_REV.1 **Widerruf**

Erläuterung: FMT_REV.1 stellt den Widerruf von Sicherheitsattributen bereit, der zu einem beliebigen Zeitpunkt durchzusetzen ist.

FMT_REV.1.1 Die TSF müssen die Fähigkeit zum Widerruf von Sicherheitsattributen, die mit Benutzern, Subjekten, Objekten und dem System selbst innerhalb des TSC verknüpft sind, auf [Zuweisung: die autorisierten identifizierten Rollen] einschränken.

FMT_REV.1.2 Die TSF müssen die folgenden Regeln

- Änderungen der Sicherheitsattribute eines Objektes werden spätestens beim nächsten Öffnen des Objektes wirksam.
- Änderungen der Sicherheitsattribute eines Benutzers werden spätestens beim nächsten Anmeldeversuch des Benutzers wirksam.
- Änderungen der globalen Sicherheitsattribute eines Systems werden spätestens beim nächsten erfolgreichen Neustart des Systems wirksam.
- In verteilten Systemen ist der Widerruf zeitnah, d.h. zum nächstmöglichen Zeitpunkt, durchzuführen.

durchsetzen.

6.1.10.5 Verfall der Sicherheitsattribute (FMT_SAE)

Erläuterung: Diese Familie betrifft die Berechtigung, Zeitbegrenzungen für die Gültigkeit von Sicherheitsattributen durchzusetzen. Dies gilt insbesondere für solche Sicherheitsattribute, bei denen eine unbegrenzte Lebensdauer zu einem unvertretbaren Risiko angesichts möglicher Attacken führt.

FMT_SAE.1 **Zeitlich begrenzte Autorisierung**

Erläuterung: FMT_SAE.1 stellt für einen autorisierten Benutzer die Berechtigung bereit, eine Verfallszeit für bestimmte Sicherheitsattribute zu spezifizieren.

FMT_SAE.1.1 Die TSF müssen die Berechtigung zur Spezifikation einer Verfallzeit für

- Benutzerkennungen
- Benutzerwählbare Authentisierungsgeheimnisse (Paßwörter)
- Tickets bzw. Credentials zur Authentisierung eines Benutzers oder Dienstes

auf die Rollen des Sicherheits-Systemtechnikers, des Sicherheitsadministrators für die Benutzerverwaltung und des Systemadministrators beschränken.

FMT_SAE.1.2 Für jedes dieser Sicherheitsattribute müssen die TSF in der Lage sein, nach Ablauf der Verfallzeit für die angezeigten Sicherheitsattribute die folgenden Aktionen

- Nach Ablauf der Gültigkeit einer Benutzerkennung darf das System keine Anmeldung des Benutzers mehr erlauben, d.h. jede Identifizierung und Authentisierung des Benutzers muß fehlschlagen.
- Das System muß beim Ablauf eines Authentisierungsgeheimnisses den Benutzer zur Änderung seines Authentisierungsgeheimnisses zwingen. Voraussetzung für die Änderung des Authentisierungsgeheimnisses ist die erfolgreiche Authentisierung des Benutzers mit dem alten Authentisierungsgeheimnis.
- Das System muß einen geschützten Mechanismus zur Verfügung stellen, der Benutzer beim Ablauf ihres Authentisierungsgeheimnisses warnt.

  Die Warnung der Benutzer vor dem Ablauf ihres Authentisierungsgeheimnisses kann geschehen entweder

  - durch Benachrichtigung des betroffenen Benutzers während eines spezifizierbaren Zeitraums vor dem Ablauf der Gültigkeit des Authentisierungsgeheimnisses

    oder
  - durch Benachrichtigung des betroffenen Benutzers bei Ablauf der Gültigkeit des Authentisierungsgeheimnisses und Zulassen einer spezifizierbaren Anzahl zusätzlicher Anmeldungen, bevor die Kennung dieses Benutzers gesperrt wird.
- Beim Ablauf eines Tickets darf das System keine Autorisierungen, die unter Vorlage dieses Tickets angefordert werden, mehr gewähren.

auszuführen.

6.1.10.6 Rollen im Sicherheitsmanagement (FMT_SMR)

Erläuterung: Diese Familie ist zur Kontrolle der Zuweisung verschiedener Rollen an Benutzer gedacht. Die Fähigkeiten dieser Rollen in Bezug auf Sicherheitsmanagement sind in den anderen Familien dieser Klasse beschrieben.

FMT_SMR.2 Einschränkungen der Sicherheitsrollen

Erläuterung: FMT_SMR.2 spezifiziert, daß es zusätzlich zu den Spezifikationen der Rollen Regeln gibt, die die Beziehung zwischen den Rollen kontrollieren.

FMT_SMR.2.1 Die TSF müssen die folgenden Rollen

- Systemadministrator
- Sicherheitsadministrator für die Rollenverwaltung
- Sicherheitsadministrator für die Benutzerverwaltung

- Auditor
- Kryptobeauftragter
- Sicherheits-Systemtechniker
- Revisor
- Operator
- Einfacher Benutzer

erhalten

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

FMT_SMR.2.3 Die TSF müssen sicherstellen, daß die folgenden Bedingungen

- Wenn ein Benutzer die Revisorrolle innehat, darf er gleichzeitig keine andere Rolle einnehmen.
- Wenn das System es erlaubt, ist die Rolle des Auditors von allen anderen administrativen Rollen zu trennen und die Einnahme einer administrativen Rolle darf nicht gleichzeitig mit der Einnahme der Rolle des Auditors geschehen.

erfüllt werden.

FMT_SMR.3 Annahme von Rollen

Erläuterung: FMT_SMR.3 erfordert die explizite Anforderung an die TSF zur Annahme einer Rolle.

Für die Rolle des einfachen Benutzers wird keine explizite Anforderung vorgesehen.

FMT_SMR.3.1 Die TSF müssen eine explizite Anforderung zur Annahme der folgenden Rollen erfordern:

- Systemadministrator
- Sicherheitsadministrator für die Rollenverwaltung
- Sicherheitsadministrator für die Benutzerverwaltung
- Auditor
- Kryptobeauftragter
- Sicherheits-Systemtechniker
- Operator
- Revisor

6.2 Anforderungen zur Vertrauenswürdigkeit

Die Anforderungen an die Vertrauenswürdigkeit eines SIZ-PP-konformen Systems sind in der nachfolgenden Tabelle wiedergegeben:

Anforderung	Bezeichnung
EAL4	Methodisch entwickelt, getestet und durchgesehen
ADV_INT.1	Modularität
ALC_FLR.3	Systematische Fehlerbehebung

Tabelle 7: Anforderungen an die Vertrauenswürdigkeit

6.2.1 Interna der EVG-Sicherheitsfunktionen (ADV_INT)

ADV_INT.1 **Modularität**

Erläuterung. Die interne Struktur des Systems soll eine Modularität aufweisen, bei der insbesondere sicherheitsrelevante Funktionen nach Möglichkeit gekapselt sind und unnötige Aufrufe zwischen den Modulen vermieden werden. Durch die Modularität wird es möglich, bei großen Systemen die Komplexität so weit zu reduzieren, daß eine Analyse der Implementierungsebene möglich wird.

ADV_INT.1.1D Der Entwickler muß Entwurf und Struktur der TSF nach einem modularen Prinzip gestalten, das unnötige Interaktionen zwischen den Modulen des Entwurfs vermeidet.

ADV_INT.1.2D Der Entwickler muß einen Architekturentwurf bereitstellen.

ADV_INT.1.1C Der Architekturentwurf muß die Module der TSF identifizieren.

ADV_INT.1.2C Der Architekturentwurf muß Zweck, Schnittstelle, Parameter und Wirkungen jedes Moduls der TSF beschreiben.

ADV_INT.1.3C Der Architekturentwurf muß beschreiben, auf welche Weise der TSF-Entwurf Module gewährleistet, die weitestgehend unabhängig sind und unnötige Interaktionen vermeiden.

6.2.2 Fehlerbehebung (ALC_FLR)

Erläuterung: In jedem System kann es vorkommen, daß nach der Auslieferung Sicherheitsmängel entdeckt werden, In solchen Fällen ist es erforderlich, daß auf Entwicklerseite ein effizientes Verfahren etabliert ist, um mit solchen Problemen umzugehen und eine Beseitigung oder Überbrückung der erkannten Schwachstelle zu ermöglichen, bevor durch sie weiterer Schaden entsteht.

ALC_FLR.3 **Systematische Fehlerbehebung**

ALC_FLR.3.1D Der Entwickler muß die Fehlerbehebungsprozeduren dokumentieren.

ALC_FLR.3.2D Der Entwickler muß eine Prozedur zur Annahme von und Reaktion auf Benutzerberichte über Sicherheitsfehler und Forderungen, diese Fehler zu beseitigen, einrichten.

ALC_FLR.3.3D Der Entwickler muß einen oder mehrere konkrete Kontaktstellen für Benutzerberichte und Anfragen zu den EVG betreffenden Sicherheitsproblemen benennen.

ALC_FLR.3.1C Die Dokumentation der Fehlerbehebungsprozeduren muß die Prozeduren beschreiben, die zur Aufzeichnung aller für jede Version des EVG gemeldeten Sicherheitsfehler angewendet werden.

ALC_FLR.3.2C Die Fehlerbehebungsprozeduren müssen erfordern, daß eine Beschreibung des Wesens und der Auswirkungen jedes Sicherheitsfehlers bereitgestellt wird, sowie des Stands der Sucher nach Korrektur dieses Fehlers.

ALC_FLR.3.3C Die Fehlerbehebungsprozeduren müssen erfordern, daß für jeden Sicherheitsfehler Aktionen zu dessen Korrektur angegeben werden.

ALC_FLR.3.4C Die Dokumentation der Fehlerbehebungsprozeduren muß die Methoden beschreiben, die für Fehlerinformationen, Korrekturen und Anleitungen für EVG-Benutzer zu Korrekturaktionen angewendet werden.

ALC_FLR.3.5C Die Prozeduren zur Behandlung gemeldeter Sicherheitsfehler müssen sicherstellen, daß sämtliche gemeldete Fehler berichtigt werden, und die EVG-Benutzer die Korrektur erhalten.

ALC_FLR.3.6C Die Prozeduren zur Behandlung gemeldeter Sicherheitsfehler müssen eine Absicherung vorsehen, daß irgendwelche Korrekturen dieser Sicherheitsfehler neue Fehler einführen.

ALC_FLR.3.7C Die Fehlerbehebungsprozeduren müssen eine Prozedur einschließen, die rechtzeitige Reaktionen für die automatische Verteilung von Sicherheitsfehlerberichten und der entsprechenden Korrekturen an die registrierten Benutzer, die von dem Sicherheitsfehler betroffen sein könnten, erfordert.

6.3 Sicherheitsanforderungen an die IT-Umgebung

Derzeit keine Anforderungen

7 Anwendungshinweise zum Schutzprofil

Derzeit keine Anmerkungen

8 Erklärungen

8.1 Einleitung

Diese Erklärungen geben zusätzliche Informationen zu den Anforderungen des Schutzprofils und analysieren die Zusammenhänge zwischen Annahmen, Bedrohungen, Sicherheitspolitik, Sicherheitszielen und Sicherheitsfunktionen. Sie unterstützen damit den Nachweis, daß das Schutzprofil vollständig, konsistent und technisch stimmig ist und sich somit zum Gebrauch als Darlegung der Anforderungen an einen oder mehrere evaluierbare EVG eignet.

Abschnitt 8.2 ”Erklärungen der Sicherheitsziele” stellt den Bezug zwischen der Sicherheitspolitik der Organisation (Abschnitt 4.3) und den Bedrohungen (Abschnitt 4.2) mit den Sicherheitszielen (Abschnitt 5) her.

In Abschnitt 8.3 ”Erklärungen der Sicherheitsanforderungen” wird der Bezug zwischen den Sicherheitszielen (aus Abschnitt 5) und den Anforderungen an Funktion und Vertrauenswürdigkeit des EVG (aus Abschnitt 6) hergestellt.

8.2 Erklärungen der Sicherheitsziele

Die CC fordern, daß die Sicherheitsziele des EVG aufgeteilt werden in Ziele, die der EVG umsetzt und solche, die die Einsatzumgebung betreffen. Sicherheitsziele sollen aussagekräftig und hilfreich sein. Zudem muß gezeigt werden, daß die Sicherheitsziele ausreichen, die erwarteten Bedrohungen abzuwehren und die Anforderungen der organisatorischen Sicherheitspolitik abzudecken.

Diese Erklärungen ignorieren den Aspekt der ”Brauchbarkeit” der Sicherheitsziele und konzentrieren sich auf den Nachweis der vollständigen Abdeckung der Bedrohungen und der Sicherheitspolitik durch die Sicherheitsziele.

8.2.1 Bedrohungen und Sicherheitsziele

In den folgenden Erklärungen wird nachgewiesen, daß die dargelegten Sicherheitsziele geeignet sind, den identifizierten Bedrohungen der Sicherheit entgegenzuwirken.

8.2.1.1 Vom EVG abzuwehrende Bedrohungen

B.Zugang **Personen erhalten logischen Zugang zum System, obwohl sie dazu nach der Sicherheitspolitik nicht befugt sind.**

Z.Zugang wirkt dieser Bedrohung direkt entgegen. Obwohl alleine dieses Ziel geeignet wäre, die Bedrohung abzuwenden, wirken auch andere Ziele dieser Bedrohung entgegen:

- Der Zugang externer Subjekte aus anderen Systemen wird durch **Z.Partner, Z.Verbindung** und **Z.KommAdmin** gewährleistet.
- **Z.Zeit-Ort** kann die Zugangsmöglichkeiten zum System und damit die Angriffsmöglichkeiten Unbefugter weiter einschränken.

- Die korrekte Nutzung der Zugangskontrollmechanismen durch die berechtigten Benutzer wird durch **Z.Benutzer** gewährleistet.
- **Z.Geheim** stellt sicher, daß die Authentisierungsgeheimnisse der Zugangskontrollmechanismen nicht in falsche Hände gelangen und dadurch einen unbefugten Zugang ermöglichen.
- Die korrekte Administration der Zugangskontrollmechanismen und der dafür erforderlichen Attribute wird durch **Z.Admin** und **Z.SysAdmin** erreicht, wobei **Z.Verantwortung** den Mißbrauch der Administrationsrechte zur Vergabe von Rechten, die der Sicherheitspolitik zuwiderlaufen protokolliert und damit bis zu einem gewissen Grad verhindert. Die Veränderung von Attributen durch unberechtigte Dritte wird durch **Z.Zugriff** verhindert.
- Die korrekte Funktion der Zugangskontrollmechanismen wird durch **Z.Software** und **Z.Betrieb** garantiert, nachdem durch **Z.Installation** die korrekte Erstinstallation der Mechanismen sichergestellt wurde.
- **Z.Fehler** und **Z.Umgehung** verhindern, daß die Zugangskontrollmechanismen ausnutzbare Schwachstellen haben oder durch manipulierte oder fehlerhafte Software umgangen werden können. Die systemexterne Manipulation der Zugangskontrollmechanismen wird durch **Z.Zutritt** und **Z.Schutz** verhindert.

B.Zugriff **Personen erhalten Zugriff auf Informationen in einem Zugriffsmodus, der nach der Sicherheitspolitik nicht erlaubt ist.**

Z.Zugriff wirkt dieser Bedrohung direkt entgegen. Die diesem Schutzprofil zugrundegelegten Zugriffskontrollmechanismen, ihre Anwendung und Administration werden jedoch auch durch weitere Ziele unterstützt, die dieser Bedrohung entgegenwirken:

- **Z.Zugang** gewährleistet, daß nur Benutzer Zugang zum System erhalten, die dem System bekannt sind und für die es Zugriffsrechte verwaltet, d.h. die Zugriffskontrolle erstreckt sich auf bekannte und vertrauenswürdige Subjekte.
- **Z.Benutzer** und **Z.Admin** stellen sicher, daß die Benutzer und Administratoren mit den Mechanismen der Rechtevergabe umgehen und die Implikationen ihres Handelns abschätzen können. Die technischen Voraussetzungen für eine Administration der Zugriffsrechte wird durch **Z.SysAdmin** geschaffen.
- Die mißbräuchliche Nutzung der Rechtevergabe wird durch **Z.Verantwortung** weitgehend verhindert. **Z.Status** ermöglicht die Kontrolle des Zustandes der Zugriffskontrollsysteme.
- Bei der rollenbasierten Zugriffskontrolle wird durch **Z.Definition** garantiert, daß die Vorgaben der Sicherheitspolitik eingehalten werden.
- Die korrekte Funktion der Zugriffskontrollmechanismen wird anfänglich durch **Z.Installation** garantiert und durch **Z.Software, Z.Fehler** und **Z.Betrieb** nachfolgend sichergestellt.
- Wenn Zugriffe über Netze erfolgen, sorgt **Z.Verbindung** für die Sicherheit der Zugriffe während der Übertragung zwischen vertrauenswürdigen Partnern. Andere Verbindungen werden durch **Z.Partner** und **Z.KommAdmin** unterbunden.

- **Z.Umgehung** verhindert, daß die Zugriffskontrollmechanismen durch manipulierte oder fehlerhafte Software umgangen werden können. Die systemexterne Manipulation der Zugriffskontrollmechanismen wird durch **Z.Zutritt** und **Z.Schutz** verhindert.

B.Fehler **Verletzungen der Sicherheitspolitik können durch Fehler in einzelnen Systemkomponenten entstehen.**

Eine wesentliche Strategie, die dieser Bedrohung entgegenwirkt, ist die Vermeidung von Fehlern. **Z.Fehler** verhindert, daß das Systemdesign ausnutzbare Schwachstellen zur Umgehung der IT-Sicherheitspolitik hat. **Z.Software** sorgt dafür, daß dieses Design im System auch nachvollziehbar umgesetzt wird und Fehler bei der Konstruktion möglichst vermieden werden.

Die zweite Strategie zielt auf das Erkennen von Fehlern und der Gewährleistung der IT-Sicherheit im Fehlerfall. **Z.Betrieb** gewährleistet die korrekte Funktion der Komponenten im Betrieb. Durch **Z.Zustand** kann auch bei Fehlern ein sicherer Betriebszustand garantiert werden.

Mittels **Z.Status** läßt sich jederzeit der aktuelle Sicherheitszustand des EVG erkennen und damit bei schweren Fehlern mittels **Z.Archiv** ein alter, sicherer Betriebszustand wiederherstellen.

B.Absturz **Der sichere Betriebszustand des Systems geht bei schweren Ausnahmefehlern verloren.**

Z.Zustand wirkt dieser Bedrohung direkt entgegen, indem die Beibehaltung eines sicheren Betriebszustandes gewährleistet wird. Durch **Z.Archiv** wird sichergestellt, daß nach einem schweren Ausnahmefehler wieder ein sicherer Betriebszustand hergestellt werden kann, um den Betrieb fortzuführen.

Flankierend wird das Auftreten solcher schweren Ausnahmefehler minimiert durch die Verhinderung von Konstruktionsfehlern über **Z.Software**, sowie die Gewährleistung des sicheren Betriebszustandes durch **Z.Betrieb**.

B.Verfügbarkeit **Berechtigte Benutzer können auf die Informationen und Ressourcen des Systems nicht zugreifen.**

Z.Verfügbarkeit wirkt dieser Bedrohung direkt entgegen. Weiterhin wirken folgende Ziele dieser Bedrohung entgegen:

- Voraussetzung für die Gewährleistung der Verfügbarkeit von Ressourcen ist die Möglichkeit ihres Managements, die durch **Z.SysAdmin** bereitgestellt wird.
- Der Bedrohung des Verfügbarkeitsverlustes durch unberechtigte Nutzung von Systemressourcen wirken **Z.Zugang** und **Z.Zugriff** entgegen.
- Ein Verfügbarkeitsverlust durch die berechtigte Nutzung von Systemressourcen wird durch **Z.Verantwortung** und **Z.Benutzer** verhindert.
- Ein Verfügbarkeitsverlust durch einen Systemabsturz wird durch **Z.Zustand**, **Z.Archiv**, **Z.Software** und **Z.Betrieb** verhindert.
- Ein Verfügbarkeitsverlust durch die Auswirkungen von Systemabstürzen wird durch **Z.Archiv** und **Z.Aufbewahrung** verhindert.

- **Z.KommAdmin** stellt sicher, daß keine Verbindungen existieren, über die die Verfügbarkeit mittels eines Denial-of-Service-Angriffs gefährdet werden kann.

B.Beweis **Sicherheitsrelevante Ereignisse werden nicht aufgezeichnet oder können dem Benutzer, der sie ausgelöst hat, nicht eindeutig zugeordnet werden.**

Dieser Bedrohung wird durch **Z.Verantwortung** direkt entgegengewirkt, da dieses Sicherheitsziel die Speicherung sämtlicher Informationen garantiert, die benötigt werden, um einen Benutzer für seine Aktionen mit dem EVG zur Verantwortung zu ziehen.

Zusätzlich dazu helfen folgende Sicherheitsziele:

- **Z.SysAdmin** stellt sicher, daß die für die Beweissicherung und Protokollierung erforderlichen Administrations- und Managementfunktionen im System vorhanden sind.
- Nach einem Systemfehler gewährleistet **Z.Archiv** die sichere Wiederherstellung der Umgebung und damit weiterhin die korrekte Funktion der Beweissicherung.
- **Z.Aufbewahrung** gewährleistet die erforderliche Aufbewahrung der Daten für die Beweissicherung.
- **Z.Umgehung** verhindert, daß die Beweissicherung umgangen werden kann.
- Durch **Z.Zugang** und **Z.Zugriff** wird verhindert, daß unbefugte Benutzer die Protokolldaten manipulieren können. Durch **Z.Verbindung** wird verhindert, daß Protokolldaten bei der Übertragung im Netz manipuliert werden können.
- Fehler in der Beweissicherung werden durch **Z.Fehler** und **Z.Software** sowie durch **Z.Betrieb** und **Z.Zustand** unterbunden.

B.Manipulation **Manipulation sicherheitsrelevanter Mechanismen ist möglich.**

Die Manipulation sicherheitsrelevanter Mechanismen könnte durch mehrere Umstände möglich werden, denen jeweils die Sicherheitsziele geeignet entgegenwirken müssen:

- **Z.Zugriff** verhindert den unbefugten Zugriff auf die sicherheitsrelevanten Objekte des Systems, die die Mechanismen und ihre Attribute enthalten. **Z.Verbindung** gewährleistet dies auch bei Netzverbindungen.
- Eine Manipulation durch ausnutzbare Schwachstellen wird durch **Z.Fehler** und **Z.Umgehung** verhindert. **Z.Software** wirkt gegen eine fehlerhafte Implementierung, die Manipulationen ermöglichen würde.
- Die Möglichkeit der Manipulation durch Lücken, die im Fehlerfall auftreten, wird durch **Z.Fehler**, **Z.Umgehung** und **Z.Software** sowie **Z.Betrieb** und **Z.Zustand** verhindert.
- Manipulationen durch Fehler in der Administration werden durch **Z.Admin** und **Z.SysAdmin** ausgeschlossen, wobei durch **Z.Installation** der korrekte Anfangszustand, von dem aus bei korrekter Administration solche Fehler ausgeschlossen werden, garantiert wird. Der sichere Systemzustand kann über **Z.Status** jederzeit nach-

geprüft werden.

- Die systemexterne Manipulation der Mechanismen wird durch **Z.Schutz** und **Z.Zutritt** verhindert.

B.Erkennen **Ereignisse während des Betriebes, die die Sicherheit des Systems verletzen, werden nicht rechtzeitig erkannt.**

Mögliche Verletzungen der Sicherheitspolitik müssen erkannt und auf ein möglichst kleines Zeitfenster reduziert werden. Dies wird wesentlich durch eine laufende Kontrolle des Systems erreicht, die durch **Z.Status** direkt unterstützt wird. Die erforderlichen Ressourcen für eine laufende Überwachung werden über **Z.SiPol** bereitgestellt. Die Verfügbarkeit der für die Kontrolle erforderlichen Daten wird über **Z.Verfügbarkeit** gewährleistet.

Voraussetzung einer Kontrolle ist die (ansonsten) sichere Funktion des Systems, die **Z.Betrieb** gewährleistet, sowie die Administration des Systems, die über **Z.Admin** und **Z.SysAdmin** sichergestellt wird.

Die Gefahr, daß Sicherheitsverletzungen trotz Kontrolle nicht erkannt werden, weil dazu keine auswertbaren Daten erzeugt wurden, wird durch **Z.Fehler** in Verbindung mit **Z.Software** verhindert.

Zur Gefahr, daß das Erkennen einer Sicherheitsverletzung wegen einer Datenmanipulation verhindert wird, vgl. **B.Manipulation**

8.2.1.2 Von der Betriebsumgebung abzuwehrende Bedrohungen

B.Installation **Das System kann in einem unsicheren Zustand ausgeliefert und installiert werden.**

Z.Installation wirkt dieser Bedrohung direkt entgegen. Durch **Z.Status**, **Z.Admin** und **Z.SysAdmin** kann der sichere Ausgangszustand verifiziert werden. Die erforderlichen Voraussetzungen im organisatorischen Bereich werden durch **Z.SiPol** geschaffen.

B.Gewalt **Durch äußere Gewalteinwirkung können sicherheitskritische Komponenten des Systems manipuliert oder außer Funktion gesetzt werden.**

Durch **Z.Schutz** wird sichergestellt, daß sicherheitskritische Systemkomponenten in gesicherten Bereichen stehen oder über andere Schutzmechanismen vor Gewalteinwirkung verfügen. Der Zutritt zu gesicherten Bereichen wird durch **Z.Zutritt** kontrolliert, so daß eine Gewalteinwirkung durch Unbefugte ausgeschlossen wird. **Z.Admin** stellt sicher, daß die Administratoren, die Zutritt zum System haben, vertrauenswürdig sind und das System nicht manipulieren.

Durch **Z.Status**, **Z.Admin** und **Z.SysAdmin** können evtl. Manipulationen z.T. erkannt werden.

B.Betrieb **Durch Fehler in Administration und Betrieb des Systems kommt es zu Verletzungen der Sicherheitspolitik.**

Z.Admin und **Z.SiPol** stellen sicher, daß Administrationsfehler durch die angemessene Ausbildung der Administratoren und ausreichende Ressourcen für sie weitgehend verhindert werden.

Durch **Z.KommAdmin** ist sichergestellt, daß dies auch auf den Bereich

der Netzverbindungen zutrifft.

Z.SysAdmin und **Z.Software** gewährleisten, daß Fehler bei der Eingabe über Plausibilitätsprüfungen weitgehend verhindert werden.

Fehler auf Benutzerseite werden wesentlich durch **Z.Benutzer** und **Z.Geheim** minimiert.

Da Fehler nicht völlig auszuschließen sind, wird durch die Ziele zur Bekämpfung von **B.Erkennen** erreicht, daß Fehler erkannt werden.

B.Rollen **Die Definition und die Zuweisung von Rollen geschieht so, daß die Sicherheitspolitik verletzt wird.**

Die Definition des Rollenmodells in Übereinstimmung mit der Sicherheitspolitik wird durch **Z.Definition** und **Z.SiPol** erreicht. Die Implementierung und Administration innerhalb des Systems wird durch **Z.Admin** und **Z.SysAdmin** gewährleistet.

8.2.1.3 Zusammenfassung

Die nachfolgende Tabelle faßt die obigen Ausführungen zusammen. Sie zeigt, daß jede der Bedrohungen durch mindestens ein Sicherheitsziel abgedeckt ist.

Bedrohung	Entgegenwirkendes Sicherheitsziel
Vom EVG abzuwehrende Bedrohungen	
B.Zugang	Z.Zugang, Z.Partner, Z.Verbindung, Z.KommAdmin, Z.Zeit-Ort, Z.Benutzer, Z.Geheim, Z.Admin, Z.SysAdmin, Z.Verantwortung, Z.Zugriff, Z.Software, Z.Betrieb, Z.Installation, Z.Fehler, Z.Umgehung, Z.Zutritt, Z.Schutz
B.Zugriff	Z.Zugriff, Z.Zugang, Z.Benutzer, Z.Admin, Z.SysAdmin, Z.Verantwortung, Z.Status, Z.Definition Z.Installation, Z.Software, Z.Fehler, Z.Betrieb, Z.Verbindung, Z.Partner, Z.KommAdmin, Z.Umgehung, Z.Zutritt, Z.Schutz
B.Fehler	Z.Fehler, Z.Software, Z.Betrieb, Z.Zustand, Z.Status, Z.Archiv
B.Absturz	Z.Zustand, Z.Archiv, Z.Software, Z.Betrieb
B.Verfügbarkeit	Z.Verfügbarkeit, Z.SysAdmin, Z.KommAdmin, Z.Zugang, Z.Zugriff, Z.Verantwortung, Z.Benutzer, Z.Zustand, Z.Archiv, Z.Software, Z.Betrieb, Z.Aufbewahrung
B.Beweis	Z.Verantwortung, Z.SysAdmin, Z.Archiv, Z.Aufbewahrung, Z.Umgehung, Z.Zugang, Z.Zugriff, Z.Verbindung, Z.Fehler, Z.Software, Z.Betrieb, Z.Zustand
B.Manipulation	Z.Zugriff, Z.Verbindung, Z.Fehler, Z.Umgehung, Z.Software, Z.Betrieb, Z.Zustand, Z.Admin, Z.SysAdmin, Z.Installation, Z.Status, Z.Schutz,

Bedrohung	Entgegenwirkendes Sicherheitsziel
	Z.Zutritt
B.Erkennen	Z.Status, Z.SiPol, Z.Verfügbarkeit, Z.Betrieb, Z.Admin, Z.SysAdmin, Z.Fehler, Z.Software
Von der Betriebsumgebung abzuwehrende Bedrohungen	
B.Installation	Z.Installation, Z.Status, Z.Admin, Z.SysAdmin, Z.SiPol
B.Gewalt	Z.Schutz, Z.Zutritt, Z.Admin, Z.Status, Z.SysAdmin
B.Betrieb	Z.Admin, Z.SiPol, Z.KommAdmin, Z.SysAdmin, Z.Software, Z.Benutzer, Z.Geheim
B.Rollen	Z.Definition, Z.SiPol, Z.Admin, Z.SysAdmin

Tabelle 8: Zuordnung der Sicherheitsziele zu den Bedrohungen

8.2.2 Abdeckung der Sicherheitspolitik durch die Sicherheitsziele

In [SIZSiArch] wurde gezeigt, daß die Sicherheitsgrundsätze der Sicherheitspolitik der Organisation vollständig durch die Sicherheitsstrategien abgedeckt werden.

Tabelle 9 zeigt nochmals, welche Sicherheitsgrundsätze die Umsetzung welcher Sicherheitsstrategie erfordern.

Grundsatz	Untergeordnete Sicherheitsstrategien
G1	S1.1, S1.2, S1.3, S1.4, S1.5, S1.6, S1.7, S1.8, S1.9, S3.14, S3.2, S3.8, S3.9, S4.4, S5.1, S5.2, S5.3, S5.4, S5.5, S5.6, S6.1
G2	S1.7, S2.1, S2.2
G3	S3.1, S3.14, S3.2, S3.3, S3.4, S3.5, S3.6, S3.7, S3.8, S3.9
G4	S3.14, S3.6, S3.7, S3.8, S3.9, S4.1, S4.2, S4.3, S4.4, S4.5, S4.6
G5	S3.2, S3.8, S3.9, S4.4, S5.1, S5.2, S5.3, S5.4, S5.5, S5.6, S6.1
G6	S4.4, S6.1, S6.2, S6.3

Tabelle 9: Sicherheitsgrundsätze und untergeordnete Sicherheitsstrategien

Nachfolgend muß daher lediglich die Abdeckung der Sicherheitsstrategien durch die Sicherheitsziele bzw. durch die diesem Schutzprofil zugrundeliegenden Annahmen überprüft werden. Der Zusammenhang der einzelnen Sicherheitsstrategien untereinander, durch die die Umsetzung einer **Sicherheitsstrategie** durch die Umsetzung anderer Sicherheitsstrategien unterstützt wird, ist in [SIZSiArch] ausführlich dargestellt.

8.2.2.1 Sicherheitsstrategien zu G1

S1.1 **Umsetzung und Einhaltung der Maßnahmen als Managementaufgabe**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies umfaßt die Verpflichtung des Managements auf die Umsetzung und Einhaltung der Sicherheitspolitik selbst.

S1.2 **Etablierung eines Verfahrens „Sicherheitsmanagement“ im Prozeßmodell des Unternehmens**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Etablierung eines Prozesses „IT-Sicherheitsmanagement“ im Prozeßmodell des Unternehmens ein.

S1.3 **Durchgängige Gewährleistung von IT-Sicherheit in neuen Anwendungssystemen / Releases**

Z.Software gewährleistet die Vertrauenswürdigkeit aller in einem SIZ-PP-konformen System zum Einsatz kommenden Softwarekomponenten. Die in diesem Schutzprofil beschriebene Vertrauenswürdigkeitsstufe, die in Erreichung dieses Ziels gefordert wird, gewährleistet, daß die erforderlichen Funktionen auch tatsächlich in den Softwarekomponenten implementiert wurden und funktionstüchtig sind.

S1.4 **Erklärung eines verbindlichen Anwendungsentwicklungsmodells für die Anwendungsentwicklung**

Z.Software stellt sicher, daß die in diesem Schutzprofil geforderte Stufe der Vertrauenswürdigkeit erreicht wurde. Diese Vertrauenswürdigkeitsstufe stellt sicher, daß das gesamte System methodisch entworfen, getestet und geprüft wurde. Die in EAL4 vorgeschriebenen Voraussetzungen ergeben zusammengenommen bereits ein eigenes Anwendungsentwicklungsmodell, das der Anforderung S1.4 entspricht.

S1.5 **Durchsetzung der IT-Sicherheit in Betrieb und Produktion**

Die Aufrechterhaltung der IT-Sicherheit in Betrieb und Produktion setzt zunächst eine sichere Ausgangsposition voraus. Diese wird durch **Z.Installation** sichergestellt.

Nach der Durchführung der korrekten Installation wird die fortlaufende Aufrechterhaltung der IT-Sicherheit dadurch erreicht, daß

- das System selbst für die Beibehaltung eines sicheren Betriebszustandes sorgt. Dies wird durch **Z.Betrieb** gewährleistet. Zusätzlich stellt **Z.Umgehung** sicher, daß die Sicherheitsfunktionen nicht umgangen werden können, so daß die Sicherheitsfunktionen tatsächlich die sicherheitsrelevanten Zustandsübergänge innerhalb des Systems kontrollieren.
- keine Fehler im System zu unsicheren Betriebszuständen führen können. Durch **Z.Fehler** wird sichergestellt, daß keine ausnutzbaren Schwachstellen im System bestehen, die solche Zustände verursachen könnten.
- die logische Funktion des Systems nicht durch physikalische Angriffe unterlaufen werden kann. Dies wird durch **Z.Schutz** und **Z.Zutritt** gewährleistet.

- im Fehlerfall ein sicherer Zustand beibehalten wird. Dies wird von **Z.Zustand** gewährleistet. Darüber hinaus stellt **Z.Archiv** sicher, daß nach nicht mehr behebbaren Fehlerzuständen auf einem gespeicherten, sicheren Systemzustand wieder aufgesetzt werden kann.

Wenn sichergestellt ist, daß das System eine unberechtigte Änderung seines sicheren Betriebszustandes erfolgreich verhindern kann, ist sicherzustellen, daß dieser sichere Betriebszustand auch durch berechtigte Aktionen nicht gefährdet wird. Dies wird erreicht durch

- eine korrekte Verwaltung des Systems. Dies wird durch **Z.SysAdmin**, **Z.KommAdmin** und **Z.Admin** gewährleistet. Soweit Benutzer für eigene Objekte administrative Tätigkeiten ausführen dürfen (z.B. Zuweisung von Zugriffsrechten), ist dies durch **Z.Benutzer** gewährleistet.
- die Gewährleistung korrekter Zugriffsrechte berechtigter Anwender auf die Ressourcen des Systems über **Z.Zugriff**. Für rollen- und gruppenbasierte Zugriffsrechte stellt **Z.Definition** die korrekte Zuordnung zu Rollen und Gruppen sicher.
- die Verhinderung des Zuganges unbefugter Subjekte zum System durch **Z.Zugang**. Der Zugang externer Subjekte aus anderen Systemen wird durch **Z.Verbindung** kontrolliert. **Z.Geheim** stellt sicher, daß die Authentisierungsgeheimnisse der Zugangskontrollmechanismen nicht in falsche Hände gelangen. **Z.Umgehung** verhindert, daß die Zugangskontrollmechanismen bei Auftreten systemexterner Fehler umgangen werden können.
- die zur Durchsetzung der IT-Sicherheit erforderlich Möglichkeit der Überprüfung des Sicherheitszustandes. Dies wird durch **Z.Admin, Z.Status** und **Z.SysAdmin** gewährleistet.

S1.6 Organisationsinterne Verdeutlichung und verbindliche Erklärung des hohen Stellenwertes der IT-Sicherheit

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S1.7 Förderung des Sicherheitsbewußtseins

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

Durch **Z.Benutzer** wird eine ausreichende Schulung aller Benutzer des Systems vorausgesetzt. Es ist unstrittig, daß eine solche Schulung auch alle sicherheitsrelevanten Aspekte des Handelns der Benutzer umfaßt. Dies trägt zur Förderung des Sicherheitsbewußtseins bei.

S1.8 Betonung des Schutzcharakters von Sicherheit

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S1.9 Verdeutlichung und Betonung des hohen Stellenwertes der IT-Sicherheit gegenüber Kunden und Partnern

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

Z.Partner stellt sicher, daß die Kooperation mit Kunden und Partnern auf elektronischem Wege nur nach Feststellung der Vergleichbarkeit der Sicherheitspolitiken erfolgen kann. Damit wird diesen der Stellenwert der IT-Sicherheit verdeutlicht.

8.2.2.2 Sicherheitsstrategien zu G2

S2.1 Herstellung der Gesetzeskonformität

Z.Verantwortung und **Z.Archiv** gewährleisten die Einhaltung der gesetzlichen Anforderungen zur Nachvollziehbarkeit und Beweisbarkeit von Transaktionen im System. Die Gesetzeskonformität dieser Funktionen wird durch die Vertrauenswürdigkeit des Systems über **Z.Software** auf der Evaluationsstufe EAL4 sichergestellt.

Für andere Bereiche außerhalb der Kontrolle des Systems gewährleistet **Z.SiPol** die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S2.2 Einflußnahme auf Gesetze und Regelungen

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

8.2.2.3 Sicherheitsstrategien zu G3

S3.1 Festlegung von Verantwortungsbereichen innerhalb der beteiligten Systeme und Netze

Z.Definition stellt die Zuweisung von Rollen und Gruppen in Übereinstimmung mit der Sicherheitspolitik sicher.

Die zusätzlich erforderlichen organisatorischen Voraussetzungen werden durch **Z.SiPol** gewährleistet.

S3.2 Gewährleistung der Integrität von Daten, Programmen und Ressourcen

Die Integrität von Daten, Programmen und Ressourcen wird dadurch erreicht, daß ausgehend von einem sicheren Betriebszustand unbefugte Manipulationen verhindert werden. Dies geschieht durch

- die Verhinderung unerlaubter Zugriffe auf die Systemressourcen. Dies wird durch **Z.Zugriff** erreicht. Die korrekte Zuteilung der Zugriffsrechte wird durch **Z.Admin, Z.Benutzer** und **Z.Definition** gewährleistet.
- die Unumgehbarkeit der Sicherheitsfunktionen. Dies gewährleistet **Z.Umgehung**.
- die Sicherstellung der Integrität während der Übertragung. Dies wird durch **Z.Verbindung** gewährleistet.
- die Gewährleistung der korrekten Funktion der Sicherheitsfunktionen. Dies wird durch **Z.Betrieb** sichergestellt.
- die Verhinderung ausnutzbarer Systemschwachstellen, durch die unbemerkte Verletzungen der Integrität von Daten und Programme erfolgen könnten. Dies gewährleistet **Z.Fehler**.

- die Verhinderung systemexterner Manipulationen. Dies wird durch **Z.Zutritt** und **Z.Schutz** erreicht.
- die Unterbindung unberechtigter Systemzugänge, über die berechtigte Änderungen an den Daten und Programmen erfolgen könnten. Dies wird durch **Z.Verbindung** in Verbindung mit **Z.KommAdmin** und **Z.Zugang** in Verbindung mit **Z.Geheim** erreicht.
- Durch **Z.Zeit-Ort** erfolgt eine weitere Beschränkung des Zugangs.
- Die Sicherstellung der Integrität von Daten und Programmen im Fehlerfall. Dies stellt **Z.Zustand** sicher.
- Die Gewährleistung der Integrität von Daten und Programmen beinhaltet auch die Möglichkeit des Nachweises der Integrität. Dieser Integritätsnachweis wird durch **Z.Admin**, **Z.SysAdmin** und **Z.Status** ermöglicht.

S3.3 Gewährleistung der Verbindlichkeit von Daten und Programmen

Die Verbindlichkeit von Daten, Programmen und Aktionen wird durch **Z.Verantwortung** in Verbindung mit der Gewährleistung der Integrität (vgl. S3.2) sichergestellt.

S3.4 Gewährleistung der Vertraulichkeit von Daten und Programmen

Die Vertraulichkeit von Daten und Programmen wird dadurch erreicht, daß ausgehend von einem sicheren Betriebszustand unbefugte Lesezugriffe auf Daten und Programmen verhindert werden. Dies geschieht durch

- die Verhinderung unerlaubter Zugriffe auf die Systemressourcen. Dies wird durch **Z.Zugriff** sichergestellt. Die korrekte Zuteilung der Zugriffsrechte wird durch **Z.Admin, Z.Benutzer** und **Z.Definition** gewährleistet.
- die Unumgehbarkeit der Sicherheitsfunktionen. Dies stellt **Z.Umgehung** sicher.
- die Gewährleistung der korrekten Funktion der Sicherheitsfunktionen. Dies wird durch **Z.Betrieb** erreicht.
- die Wahrung der Vertraulichkeit während der Übertragung. Dies wird durch **Z.Verbindung** gewährleistet.
- die Verhinderung ausnutzbarer Systemschwachstellen, durch die ein unbemerkter Zugriff erfolgen könnte. Dies stellt **Z.Fehler** sicher.
- die Verhinderung systemexterner Manipulationen, die das Ziel haben, in den Besitz geschützter Daten und Programme zu gelangen. Dies stellen **Z.Schutz** und **Z.Zutritt** sicher.
- die Unterbindung unberechtigter Systemzugänge, über die berechtigte Zugriffe Daten und Programmen erfolgen könnten. Dies wird durch **Z.Verbindung** und **Z.Zugang** in Verbindung mit **Z.Geheim** gewährleistet. Durch **Z.Zeit-Ort** erfolgt eine weitere Beschränkung des Zugangs.

S3.5 Gewährleistung der Verfügbarkeit von Daten und Programmen

Dies wird direkt durch **Z.Verfügbarkeit** erreicht.

S3.6 **Funktionstrennung**

Z.Definition gewährleistet die Definition und Zuweisung von Rollen und Gruppen in Übereinstimmung mit der geltenden Sicherheitspolitik. Dies schließt die Funktionstrennung mit ein.

Die erforderlichen Authentisierungsverfahren werden über **Z.Zugang** bereitgestellt.

S3.7 **Rollen- und Aufgabenidentifizierung**

Durch **Z.Verantwortung** wird sichergestellt, daß die Aufgaben und Rollen eines berechtigten Benutzers jederzeit erkennbar und nachvollziehbar sind.

S3.8 **Zugriffskontrolle zu Ressourcen**

Z.Zugriff setzt diese Sicherheitsstrategie direkt um, wobei die korrekte Funktion der Zugriffskontrolle durch **Z.Definition, Z.Benutzer** und **Z.Admin** gewährleistet wird. **Z.Umgehung** stellt sicher, daß die Zugriffskontrolle nicht umgangen werden kann, also immer in Kraft ist. **Z.Verbindung** gewährleistet, daß auch bei Zugriffen von externen Rechnern die Sicherheitspolitik beachtet wird.

S3.9 **Identifikation aller Kommunikationspartner**

Z.Zugang schließt den Systemzugang für unberechtigte Personen aus. Durch **Z.Verantwortung** in Verbindung mit **Z.Zugang** wird erzwungen, daß alle berechtigten Benutzer eindeutig identifiziert werden.

Z.Zugang erzwingt neben einer eindeutigen Identifizierung auch die dazugehörende Authentisierung aller Subjekte. Durch **Z.Geheim** wird verhindert, daß unbefugte Benutzer unter der Kennung berechtigter Benutzer in das System eindringen können.

Durch **Z.Zustand** wird verhindert, daß im Fehlerfall Benutzer unberechtigten Systemzugang erhalten können.

Über **Z.Verbindung, Z.KommAdmin** und **Z.Partner** wird gewährleistet, daß keine Verbindungen zu nicht vertrauenswürdigen Systemen hergestellt werden können. Dies impliziert eine Systemauthentisierung.

S3.14 **Archivierung und Nachvollziehbarkeit**

Die Sicherheitsstrategie zur Archivierung und Nachvollziehbarkeit wird direkt über **Z.Archiv** und **Z.Verantwortung** in Verbindung mit **Z.Zugang**. abgedeckt.

8.2.2.4 Sicherheitsstrategien zu G4

S4.1 **Vermeidung von Interessenskonflikten für Mitarbeiter durch geeignete organisatorische und technische Maßnahmen**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S4.2 **Nutzung von Systemen nur nach erfolgreicher Identifikation und Authentisierung**

Diese Sicherheitsstrategie wird direkt durch **Z.Zugang** abgedeckt. Zusätzlich wird durch **Z.Umgehung** sichergestellt, daß die Identifikation und Authentisierung nicht umgangen werden können. **Z.Verbindung** bewirkt, daß

bei Verbindungen mit anderen Systemen dieses authentisiert ist und die gleiche Sicherheitspolitik für seine Benutzer durchsetzt.

S4.3 Klare Beschreibung der Sicherheitspolitik

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S4.4 Mitarbeitereinsatz

Die organisatorischen Bestandteile dieser Sicherheitsstrategie deckt **Z.SiPol** ab.

Weiterhin wird durch **Z.Definition** die korrekte Definition von Gruppen und Rollen und durch **Z.Status** ihre Erkennbarkeit im System gewährleistet.

S4.5 Festlegung von Absicherungsverfahren

Diese Sicherheitsstrategie befaßt sich mit Ausnahmesituationen, die oftmals nicht durch Konzepte, wie sie das IT-System bereitstellt, abgedeckt werden können. Sie liegen daher größtenteils außerhalb der Grenzen des IT-Systems und werden über die Umsetzung der Sicherheitspolitik im organisatorischen Bereich abgedeckt, die über **Z.SiPol** gewährleistet ist.

Soweit es sich um Maßnahmen handelt, die im IT-System selbst umgesetzt werden, sorgt **Z.Admin** für die korrekte Umsetzung der Maßnahmen.

S4.6 Risikobewertung einzelner Aufgaben und Funktionen

Z.Software stellt sicher, daß für die vom System bereitgestellten Sicherheitsfunktionen eine Bewertung der Schwachstellen im Design und Betrieb des Systems durchgeführt wurde. Für andere Aufgaben und Funktionen außerhalb der Systemgrenze wird diese Sicherheitsstrategie über **Z.SiPol** abgedeckt.

8.2.2.5 Sicherheitsstrategien zu G5

S5.1 Umsetzung der Anforderungen an Nachvollziehbarkeit, Beweispflicht und Revisionsfähigkeit, die sich aus Gesetzen, Regelungen und Anforderungen der Sparkassenorganisation ergeben

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

Die Sicherheitsstrategie zur Nachvollziehbarkeit wird direkt über **Z.Archiv** und **Z.Verantwortung** in Verbindung mit **Z.Zugang** abgedeckt.

S5.2 Festlegung organisationseigener Sicherheitsanforderungen bezüglich Nachvollziehbarkeit, Beweispflicht und Revisionsfähigkeit

Die Festlegung organisationseigener Sicherheitsanforderungen wird über **Z.SiPol** gewährleistet. Die Umsetzung dieser Anforderungen durch **Z.Admin**, **Z.KommAdmin**, **Z.Verantwortung** und **Z.Archiv** abgedeckt.

S5.3 Ermittlung und Erzeugung von Daten zur Nachvollziehbarkeit

Die Sicherheitsstrategie zur Nachvollziehbarkeit wird direkt über **Z.Archiv** und **Z.Verantwortung** in Verbindung mit **Z.Zugang**. abgedeckt.

S5.4 **Bereitstellung und Schutz von Revisionsdaten**

Die Sicherheitsstrategie zur Archivierung und Nachvollziehbarkeit wird direkt über **Z.Archiv** und **Z.Verantwortung** in Verbindung mit **Z.Zugang**. abgedeckt.

S5.5 **Sichere Aufbewahrung der beweisrelevanten Informationen**

Die das System betreffenden Anforderungen dieser Sicherheitsstrategie werden direkt über **Z.Archiv** in Verbindung mit **Z.Verantwortung** abgedeckt. Externe organisatorische Maßnahmen werden von **Z.SiPol** und **Z.Aufbewahrung** erfaßt

S5.6 **Unleugbarkeit aller geschäftlichen Transaktionen**

Die Verbindlichkeit von Daten, Programmen und Aktionen wird durch **Z.Verantwortung** in Verbindung mit der Gewährleistung der Integrität (vgl. S3.2) sichergestellt.

8.2.2.6 Sicherheitsstrategien zu G6

S6.1 **Beschreibung der Sicherheitspolitik mit allen zugehörigen Aspekten**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S6.2 **Regelmäßiger Nachweis und Dokumentation der Einhaltung von Standards und Regelwerken**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

S6.3 **Fortschreibung und Anpassung der Standards und Regelwerke**

Z.SiPol gewährleistet die Umsetzung der Sicherheitspolitik im organisatorischen Bereich. Dies schließt die Umsetzung dieses Zieles mit ein.

Soweit systemrelevante Dokumentation von dieser Sicherheitsstrategie betroffen ist, wird sie über **Z.Software** über EAL4 abgedeckt.

Die folgende Tabelle faßt die Zuordnung der Sicherheitsziele zu den Sicherheitsstrategien nochmals zusammen:

Sicherheits-strategie	Sicherheitsziel
S1.1	Z.SiPol
S1.2	Z.SiPol
S1.3	Z.Software
S1.4	Z.Software
S1.5	Z.Installation, Z.Betrieb, Z.Umgehung, Z.Fehler, Z.Schutz, Z.Zutritt, Z.Zustand, Z.Archiv, Z.SysAdmin, Z.KommAdmin, Z.Admin, Z.Benutzer, Z.Zugriff, Z.Definition, Z.Zugang, Z.Verbindung, Z.Geheim, Z.Status
S1.6	Z.SiPol

Sicherheits-strategie	Sicherheitsziel
S1.7	Z.SiPol, Z.Benutzer
S1.8	Z.SiPol
S1.9	Z.SiPol, Z.Partner
S2.1	Z.Verantwortung, Z.Archiv, Z.Software, Z.SiPol
S2.2	Z.SiPol
S3.1	Z.Definition, Z.SiPol
S3.2	Z.Zugriff, Z.Admin, Z.Benutzer, Z.Definition, Z.Umgehung, Z.Verbindung, Z.Betrieb, Z.Fehler, Z.Zutritt, Z.Schutz, Z.KommAdmin, Z.Zugang, Z.Geheim, Z.Zeit-Ort, Z.Zustand, Z.SysAdmin, Z.Status
S3.3	Z.Verantwortung, Z.Zugriff, Z.Admin, Z.Benutzer, Z.Definition, Z.Umgehung, Z.Verbindung, Z.Betrieb, Z.Fehler, Z.Zutritt, Z.Schutz, Z.KommAdmin, Z.Zugang, Z.Geheim, Z.Zeit-Ort, Z.Zustand, Z.SysAdmin, Z.Status
S3.4	Z.Zugriff, Z.Admin, Z.Benutzer, Z.Definition, Z.Umgehung, Z.Betrieb, Z.Verbindung, Z.Fehler, Z.Schutz, Z.Zutritt, Z.Zugang, Z.Geheim, Z.Zeit-Ort
S3.5	Z.Verfügbarkeit
S3.6	Z.Definition, Z.Zugang
S3.7	Z.Verantwortung
S3.8	Z.Zugriff, Z.Definition, Z.Benutzer, Z.Admin, Z.Umgehung, Z.Verbindung
S3.9	Z.Zugang, Z.Verantwortung, Z.Geheim, Z.Zustand, Z.Verbindung, Z.KommAdmin, Z.Partner
S3.14	Z.Archiv, Z.Verantwortung, Z.Zugang
S4.1	Z.SiPol
S4.2	Z.Zugang, Z.Umgehung, Z.Verbindung
S4.3	Z.SiPol
S4.4	Z.SiPol, Z.Definition, Z.Status
S4.5	Z.SiPol, Z.Admin
S4.6	Z.Software, Z.SiPol
S5.1	Z.SiPol, Z.Archiv, Z.Verantwortung, Z.Zugang
S5.2	Z.SiPol, Z.Admin, Z.KommAdmin, Z.Verantwortung, Z.Archiv
S5.3	Z.Archiv, Z.Verantwortung, Z.Zugang
S5.4	Z.Archiv, Z.Verantwortung, Z.Zugang

Sicherheits-strategie	Sicherheitsziel
S5.5	Z.Archiv, Z.Verantwortung, Z.Aufbewahrung, Z.SiPol
S5.6	Z.Verantwortung, Z.Zugriff, Z.Admin, Z.Benutzer, Z.Definition, Z.Umgehung, Z.Verbindung, Z.Betrieb, Z.Fehler, Z.Zutritt, Z.Schutz, Z.KommAdmin, Z.Zugang, Z.Geheim, Z.Zustand, Z.SysAdmin, Z.Status
S6.1	Z.SiPol
S6.2	Z.SiPol
S6.3	Z.SiPol, Z.Software

Tabelle 10: Zuordnung der Sicherheitsziele zu den Sicherheitsstrategien

8.2.3 Bezug zwischen Sicherheitszielen und Annahmen

Gemäß der Definition in Abschnitt 5.2 sind alle Annahmen direkt in Sicherheitsziele der Betriebsumgebung umgesetzt. Es ist daher nicht notwendig, den Bezug zwischen Sicherheitszielen und Annahmen noch einmal in einer Tabelle zu erläutern.

8.2.4 Vollständigkeit der Abdeckung

Die nachfolgende Tabelle zeigt als Umkehrabbildung von Tabelle 8 und Tabelle 10, daß die vorhandenen Sicherheitsziele so gewählt sind, daß sie die Sicherheitsgrundsätze und Bedrohungen abdecken und keine Sicherheitsziele vorhanden sind, die keiner Bedrohung oder keinem Sicherheitsgrundsatz zugeordnet werden können:

Sicherheitsziel	Sicherheitsstrategie	Bedrohung
Z.Zugang	S1.5, S3.2, S3.3, S3.4, S3.6, S3.9, S3.14, S4.2, S5.1, S5.3, S5.4, S5.6	B.Zugang, B.Zugriff, B.Verfügbarkeit, B.Beweis
Z.Zugriff	S1.5, S3.2, S3.3, S3.4, S3.8, S5.6	B.Zugang, B.Zugriff, B.Verfügbarkeit, B.Beweis, B.Manipulation
Z.Archiv	S1.5, S2.1, S3.14, S5.1, S5.2, S5.3, S5.4, S5.5	B.Fehler, B.Absturz, B.Verfügbarkeit, B.Beweis
Z.Verantwortung	S2.1, S3.3, S3.7, S3.9, S3.14, S5.1, S5.2, S5.3, S5.4, S5.5, S5.6	B.Zugang, B.Zugriff, B.Verfügbarkeit, B.Beweis
Z.Zeit-Ort	S3.2, S3.3, S3.4	B.Zugang
Z.Umgehung	S1.5, S3.2, S3.3, S3.4, S3.8, S4.2, S5.6	B.Zugang, B.Zugriff, B.Beweis, B.Manipulation

Sicherheitsziel	Sicherheitsstrategie	Bedrohung
Z.Fehler	S1.5, S3.2, S3.3, S3.4, S5.6	B.Zugang, B.Zugriff, B.Fehler, B.Beweis, B.Manipulation, B.Erkennen
Z.SysAdmin	S1.5, S3.2, S3.3, S5.6	B.Zugang, B.Zugriff, B.Verfügbarkeit, B.Beweis, B.Manipulation, B.Erkennen, B.Installation, B.Gewalt, B.Betrieb, B.Rollen
Z.Betrieb	S1.5, S3.2, S3.3, S3.4, S5.6	B.Zugang, B.Zugriff, B.Fehler, B.Absturz, B.Verfügbarkeit, B.Beweis, B.Manipulation, B.Erkennen
Z.Status	S1.5, S3.2, S3.3, S4.4, S5.6	B.Zugriff, B.Fehler, B.Manipulation, B.Erkennen, B.Installation, B.Gewalt
Z.Verfügbarkeit	S3.5	B.Verfügbarkeit, B.Erkennen
Z.Zustand	S1.5, S3.2, S3.3, S3.9, S5.6	B.Fehler, B.Absturz, B.Verfügbarkeit, B.Beweis, B.Manipulation
Z.Verbindung	S1.5, S3.2, S3.3, S3.4, S3.8, S3.9, S4.2, S5.6	B.Zugang, B.Zugriff, B.Beweis, B.Manipulation,
Z.Software	S1.3, S1.4, S2.1, S4.6, S6.3	B.Zugang, B.Zugriff, B.Fehler, B.Absturz, B.Verfügbarkeit, B.Beweis, B.Manipulation, B.Erkennen, B.Betrieb
Z.Installation	S1.5	B.Zugang, B.Zugriff, B.Manipulation, B.Installation
Z.Definition	S1.5, S3.1, S3.2, S3.3, S3.4, S3.6, S3.8, S4.4, S5.6	B.Zugriff, B.Rollen
Z.Geheim	S1.5, S3.2, S3.3, S3.4, S3.9, S5.6	B.Zugang, B.Betrieb
Z.Aufbewahrung	S5.5	B.Verfügbarkeit, B.Beweis
Z.KommAdmin	S1.5, S3.2, S3.3, S3.9, S5.2, S5.6	B.Zugang, B.Zugriff, B.Betrieb, B.Verfügbarkeit
Z.Zutritt	S1.5, S3.2, S3.3, S3.4, S5.6	B.Zugang, B.Zugriff, B.Manipulation, B.Gewalt
Z.Schutz	S1.5, S3.2, S3.3, S3.4, S5.6	B.Zugang, B.Zugriff, B.Manipulation, B.Gewalt
Z.Admin	S1.5, S3.2, S3.3, S3.4, S3.8, S4.5, S5.2, S5.6	B.Zugang, B.Zugriff, B.Manipulation, B.Erkennen,

Sicherheitsziel	Sicherheitsstrategie	Bedrohung
		B.Installation, B.Gewalt, B.Betrieb, B.Rollen
Z.Benutzer	S1.5, S1.7, S3.2, S3.3, S3.4, S3.8, S5.6	B.Zugang, B.Zugriff, B.Verfügbarkeit, B.Betrieb
Z.Partner	S1.9, S3.9	B.Zugang, B.Zugriff
Z.SiPol	S1.1, S1.2, S1.6, S1.7, S1.8, S1.9, S2.1, S2.2, S3.1, S4.1, S4.3, S4.4, S4.5, S4.6, S5.1, S5.2, S5.5, S6.1, S6.2, S6.3	B.Erkennen, B.Installation, B.Betrieb, B.Rollen

Tabelle 11: Zuordnung von Sicherheitsstrategien und Bedrohungen zu den Sicherheitszielen

8.3 Erklärungen der Sicherheitsanforderungen

Aus den CC sind Komponenten auszuwählen, deren definierte Sicherheitsanforderungen an die Funktion und die Vertrauenswürdigkeit des EVG geeignet sind, alle Sicherheitsziele für den EVG und für die Umgebung umzusetzen. Es ist zu zeigen, daß die getroffene Auswahl dieser Komponenten vollständig und konsistent ist.

8.3.1 Sicherheitsziele und Sicherheitsanforderungen

In den folgenden Erklärungen wird nachgewiesen, daß die ausgewählten Sicherheitsanforderungen an die Funktion und die Vertrauenswürdigkeit des EVG geeignet sind, die aufgeführten Sicherheitsziele für den EVG und für die Umgebung vollständig und konsistent umzusetzen.

8.3.1.1 Sicherheitsziele für den EVG

Z.Zugang

Die Komponenten **FIA_UID.2** und **FIA_UAU.2** fordern eine Identifikation bzw. eine Authentisierung jedes Benutzers des EVG vor jeder weiteren Interaktion mit dem EVG. Die Anforderungen der Komponenten **FIA_UAU.4**, **FIA_UAU.5**, **FIA_UAU.6** und **FIA_UAU.7** präzisieren die verwendeten Mechanismen zur Authentisierung der Benutzer.

Durch **FTP_TRP.1** wird ein vertrauenswürdiger Pfad zur Übertragung der Anmeldungsinformationen zwischen Benutzer und EVG bereitgestellt, der sicherstellt, daß diese Informationen Dritten nicht sichtbar gemacht werden. Zusätzlich garantiert **FPT_RPL.1**, daß Wiedereinspielungen von eventuell aufgezeichneten Daten erkannt werden.

Die in **FIA_ATD.1** definierten Benutzerattribute erlauben Einschränkungen des logischen Zugangs zum EVG. Einschränkungsmöglichkeiten des logischen Zuganges werden ebenso durch **FTA_TSE.1** garantiert.

Durch **FMT_SAE.1** wird gewährleistet, daß Zugangsberechtigungen eine zeitlich begrenzte Gültigkeit haben können und nur innerhalb dieser Gül-

tigkeitsdauer logischen Zugang zum EVG gestatten. Vorgaben für Gültigkeitsdauern sind in **FMT_MSA.3** definiert. **FMT_REV.1** stellt sicher, daß Zugangsberechtigungen widerrufen werden können.

Versuchen unbefugte Benutzer mehrfach erfolglos, sich logischen Zugang zum EVG zu verschaffen, greifen die Abwehrmaßnahmen der Komponente **FIA_AFL.1**.

Die von Komponente **FIA_SOS.1** definierten Qualitätsmetriken für Authentisierungsgeheimnisse erschweren das Erraten oder Ausprobieren von Authentisierungsgeheimnissen befugter Benutzer durch Unbefugte.

Bei Abwesenheit von berechtigten Benutzern kann deren – nach **FTA_MCS.1** - einzige interaktive Sitzung sowohl vom EVG als auch vom Benutzer gesperrt und damit für Unbefugte unzugänglich gemacht werden. Dies wird von den Sicherheitsanforderungen der Komponenten **FTA_SSL.1** und **FTA_SSL.2** garantiert.

Durch **FPT_PHP.3** wird sichergestellt, daß materielle Angriffe auf den EVG nicht dazu führen können, daß Unbefugte einen logischen Zugang erhalten.

Z.Zugriff

Durch die Auswahl der Komponenten der Klasse FCS (**FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.3** und **FCS_COP.1**) wird die Verwendung kryptographischer Verfahren zur Verhinderung unberechtigter Benutzerzugriffe auf Informationen ermöglicht.

Die Zugriffskontrollpolitiken DAC und RBAC, die in den Komponenten **FDP_ACC.1** und **FDP_ACF.1** näher spezifiziert sind, bestimmen und regeln die Zugriffsberechtigungen von Benutzern auf Informationen innerhalb des EVG. Die hierzu von den Benutzern benötigten Sicherheitsattribute ergeben sich aus den Anforderungen aus **FIA_ATD.1**. Die Definition der Rollen für die Zugriffskontrollpolitik RBAC finden sich in den Komponenten **FMT_SMR.1** und **FMT_SMR.2**.

Zugriffsberechtigungen können mittels **FMT_REV.1** wieder entzogen werden.

Die Komponente **FIA_UID.2** gewährleistet die Identifikation jedes Benutzers. Durch **FIA_USB.1** werden auch alle für den Benutzer agierenden Subjekte eindeutig mit dem Benutzer verknüpft und unterliegen somit ebenfalls der für den Benutzer geltenden Zugriffsregelung. Sofern erforderlich, kann vor dem Zugriff auf Informationen nach **FIA_UAU.6** eine Wiederauthentisierung des Benutzers vom System verlangt werden.

Die Komponenten **FTA_MCS.1, FTA_SSL.1** und **FTA_SSL.2** stellen sicher, daß die einzige interaktive Benutzersitzung und die mit ihr verarbeiteten Informationen bei Abwesenheit des Benutzers durch Sperren vor dem Zugriff anderer Benutzer geschützt werden kann.

Werden Daten zwischen dem EVG und einem entfernten IT-System übertragen, gewährleisten die Anforderungen aus **FDP_UCT.1** und **FDP_UIT.1**, daß die übertragenen Daten vor Preisgabe an unbefugte geschützt sind.

Durch **FDP_RIP.2** wird garantiert, daß Benutzern bei Zuteilung die vorhergehenden Informationsinhalte der zugeteilten Betriebsmittel nicht

mehr zur Verfügung stehen.

FPT_PHP.3 stellt sicher, daß vorhandene Zugriffskontrollen durch materielle Angriffe auf den EVG nicht außer Kraft gesetzt werden können.

Durch **FPT_RPL.1** wird verhindert, daß sich Benutzer durch Wiedereinspielen von Authentisierungsdaten zugriffsberechtigter Benutzer unberechtigten Zugriff auf Informationen verschaffen.

FAU_SAR.2 beschränkt die Durchsicht der Protokollaufzeichnungen auf die dazu berechtigten Personen. **FAU_STG.2** stellt sicher, daß die Protokollaufzeichnungen nicht durch Unbefugte gelöscht oder modifiziert werden können.

FMT_MOF.1 enthält Anforderungen zur Einschränkung des Zugriffs auf konfigurierbare Sicherheitsfunktionen des EVG. Durch **FMT_MTD.1, FMT_MTD.2, FMT_MSA.1** und **FMT_MSA.3** werden die Modifikation und die Initialisierung von Sicherheitsattributen und anderer sicherheitsrelevanter Daten der Sicherheitsfunktionen auf die dazu jeweils berechtigten Benutzer festgelegt.

Z.Archiv

FDP_SDI.2 stellt die Erkennbarkeit von Integritätsfehlern und damit die Fähigkeit zur Erkennung der Notwendigkeit einer Einleitung von Wiederherstellungsmaßnahmen bereit. Desweiteren können mögliche Integritätsfehler in archivierten und wiedereingespielten Daten erkannt werden.

FPT_RCV.1 gewährleistet den Übergang des EVG in einen abgesicherten Wartungszustand, der die kontrollierte, manuelle Wiederherstellung von Informationen aus Archiven ermöglicht.

Durch Auswahl der Komponenten **FPT_ITA.1, FPT_ITC.1** und **FPT_ITI.1** wird sichergestellt, daß die bei Archivierung zu vertrauenswürdigen IT-Produkten übertragenen Daten bezüglich der Verfügbarkeit, Integrität und Vertraulichkeit geschützt sind. Die Komponenten **FDP_UIT.1** und **FDP_UCT.1** gewährleisten ebenfalls die Integrität und Vertraulichkeit der bei Archivierung und Wiederherstellung übertragenen Benutzerdaten.

Z.Verantwortung

Durch die Komponenten **FAU_GEN.1** und **FAU_GEN.2** wird die Protokollierung der sicherheitsrelevanten Aktionen der Benutzer mit Verknüpfung zur Identität des jeweiligen Benutzers des EVG sichergestellt. Zeitstempel nach **FPT_STM.1** stellen dabei den zeitlichen Bezug her.

Die Auswahl der von der Sicherheitsprotokollierung zu protokollierenden Ereignisse, die Analyse der Protokollinformationen, die Durchsicht der Sicherheitsprotokollierung und der Schutz vor Protokolldaten-Verlust ist durch die Anforderungen der Komponenten **FAU_SEL.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.2** und **FAU_STG.4** spezifiziert. Durch die automatische Reaktion der Sicherheitsprotokollierung nach **FAU_ARP.1** können potentielle Sicherheitsverletzungen erkannt und vereitelt werden.

Die Protokollinformationen sind durch die Zugriffskontrollpolitiken DAC und RBAC nach **FDP_ACC.1** und **FDP_ACF.1** vor unbefugter Manipulation geschützt. Nach **FMT_MTD.1** und **FMT_MTD.2** können nur Inhaber spezieller Rollen die Protokollinformationen verwalten und die Größe der Protokollierungsdatei verändern. Diese Rollen müssen aufgrund der

Komponente **FMT_SMR.3** explizit und damit nachweisbar angefordert werden.

Durch **FIA_UID.2, FIA_USB.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6** und **FIA_UAU.7** wird garantiert, daß jeder Benutzer eindeutig identifiziert, authentisiert und ggf. wiederauthentisiert wird und daß alle Subjekte, die für einen Benutzer agieren, eindeutig mit dessen Identität verknüpft sind.

Benutzer können erkennen, ob in ihrer Abwesenheit Aktionen unter ihrer Benutzerkennung stattgefunden haben, da ihnen bei der Anmeldung nach **FTA_TAH.1** der Zeitpunkt der Einrichtung der letzten interaktiven Sitzung angezeigt wird. Diese Komponente verhindert gleichzeitig, daß Benutzer behaupten, der mögliche Mißbrauch ihrer Benutzerkennungen sei ihnen nicht mitgeteilt worden.

Die in **FIA_SOS.1** spezifizierten Qualitätsmetriken für Authentisierungsgeheimnisse gewährleisten einen ausreichenden Schutz gegen Erraten der Authentisierungsgeheimnisse der Benutzer durch Unbefugte und unterstützen damit die Eindeutigkeit der Verknüpfung von Benutzeraktivitäten zur Identität des agierenden Benutzers.

Durch die Begrenzung auf eine interaktive Benutzersitzung gemäß Komponente **FTA_MCS.1** können Zeit und Ort jeder Benutzeraktion eindeutig der Benutzeridentität zugeordnet werden.

Die Nichtabstreitbarkeit einzelner von den Benutzern durchgeführten Aktionen wird durch die Komponenten **FCO_NRO.1** und **FCO_NRR.1** gewährleistet.

Benutzer sind nach **FPT_RPL.1** nicht in der Lage, durch Wiedereinspielen von Daten, die mit einer anderen Benutzeridentität verknüpft sind, sicherheitsrelevante Aktionen zu Lasten oder zu Gunsten dieser Benutzeridentität auszulösen.

Z.Zeit-Ort Die Durchsetzung dieses Zieles wird durch Auswahl der Komponente **FTA_TSE.1** gewährleistet.

Für jeden Benutzer existieren nach **FIA_ATD.1** Sicherheitsattribute, die die erlaubten Login-Zeiten und Zugangspunkte beinhalten. Auf Grundlage dieser Sicherheitsattribute kann der Zugang in Abhängigkeit vom Benutzer verweigert werden. Nach den Anforderungen der Komponente **FTA_LSA.1** kann der Umfang der Aktivitäten für jeden Benutzer nach dessen erfolgreicher Anmeldung aufgrund dieser ihm zugeordneten Sicherheitsattribute eingeschränkt werden.

Zur Feststellung des Zeitpunktes eines Loginversuchs benötigt der EVG die verläßlichen Zeitstempel, die von der Komponente **FPT_STM.1** bereitgestellt werden.

Das Management der zeitlichen Begrenzung von Zugangsberechtigungen durch Angabe einer Gültigkeitsdauer für einzelne Benutzerkennungen wird in **FMT_SAE.1** spezifiziert.

Z.Umgehung Die Auswahl der Evaluationsstufe **EAL4** für den EVG macht bereits deutlich, daß dem EVG ein ausreichendes Vertrauen bezüglich der Unumgehbarkeit der Sicherheitsfunktionen entgegengebracht wird. Die Aus-

wahl der Komponente **FPT_RVM.1** stellt die Unumgehbarkeit aller Sicherheitsfunktionen des EVG sicher.

Die Bereichsseparierung nach Komponente **FPT_SEP.2** gewährleistet den Schutz der Sicherheitsfunktionen des EVG vor Eingriffen und Manipulationen durch nicht vertrauenswürdige Subjekte.

Durch die Komponente **FPT_PHP.3** wird garantiert, daß auch materielle Angriffe nicht zu einer Umgehbarkeit von Sicherheitsmechanismen führen können.

Den Benutzern des EVG wird durch **FTP_TRP.1** ein vertrauenswürdiger Pfad zur Übertragung der Anmeldungsinformationen bereitgestellt, der nicht umgangen werden kann. Für die Übertragung sicherheitsrelevanter Informationen steht durch **FTP_ITC.1** zudem ein vertrauenswürdiger Kanal zur Verfügung, der nicht umgehbar ist.

Erfolglose Versuche, die Sicherheitsfunktionen der Identifikation und Authentisierung zu umgehen, werden von **FIA_AFL.1** erkannt und verarbeitet.

Jede Wiedereinspielung von Daten, die die Sicherheitsfunktionen umgehen könnte, wird durch die Anforderungen aus **FPT_RPL.1** erkannt. Bei der Verwendung von Authentisierungsmechanismen für einmaligen Gebrauch verhindert die Komponente **FIA_UAU.4** eine mehrfache Benutzung der Authentisierungsdaten.

Die Vertraulichkeit und Integrität von übertragenen Informationen wird durch **FPT_ITC.1** und **FPT_ITI.1** gewährleistet. Die Umgehung von Sicherheitsfunktionen durch Modifikation oder Aufzeichnung von übertragenen Informationen wird somit verhindert.

Die Umgehung der Protokollierung sicherheitsrelevanter Aktionen durch nachträgliche Modifikation, Löschen oder Provokation eines Überlaufs der zugehörigen Protokolldateien wird durch **FAU_STG.2** und **FAU_STG.4** verhindert.

Z.Fehler

Die Auswahl der Evaluationsstufe **EAL4** für den EVG macht bereits deutlich, daß dem EVG ein ausreichendes Vertrauen bezüglich Fehlerfreiheit in Design, Implementierung und Betrieb entgegengebracht wird. Sämtliche Schnittstellen zwischen den unabhängigen Modulen des EVG sind nach **ADV_INT.1** beschrieben. Gemäß **ALC_FLR.3** muß der Entwickler des EVG auch nachweisen, daß erkannte Fehler umgehend behoben wurden und zukünftig systematisch behebbar sind.

Der sichere Umgang mit kryptographischen Verfahren und Schlüsseln ist durch die Anforderungen der Komponenten **FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3** und **FCS_CKM.4** sichergestellt.

Erfolglose Versuche, die Sicherheitsfunktionen der Identifikation und Authentisierung zu umgehen, werden von **FIA_AFL.1** erkannt und verarbeitet und stellen keine ausnutzbare Schwachstelle dar.

Durch die Spezifikation einer Qualitätsmetrik für Authentisierungsgeheimnisse nach **FIA_SOS.1** wird einer potentiellen Schwachstelle schwacher Paßwörter entgegengewirkt.

Durch die Zuweisung unterschiedlicher Authentisierungsmechanismen

zu unterschiedlichen Diensten des EVG nach **FIA_UAU.5** wird die potentielle Ausnutzbarkeit der Schwachstelle Authentisierungsgeheimnis auf solche Bereiche und Aktionen beschränkt, die nicht geeignet sind, die Sicherheit des EVG wesentlich zu gefährden.

Schwachstellen aufgrund unsicherer Konfiguration von Sicherheitsattributen sind laut Anforderung **FMT_MSA.2** nicht möglich. Durch Spezifikation von Verfallzeiten für Sicherheitsattribute nach **FMT_SAE.1** wird sichergestellt, daß Sicherheitsattribute nach einer eventuellen Komprommitierung nur für eine begrenzte Zeitspanne für Angriffe mißbraucht werden können.

Bei Abwesenheit des Benutzers einer interaktiven Sitzung kann nach **FTA_SSL.1** der EVG die Benutzerkennung sperren und somit Angriffe, die von Dritten unter Nutzung dieser Benutzerkennung ausgehen könnten, unterbinden.

Die Sicherung der Integrität von übertragenen Daten gemäß der Anforderung der Komponente **FPT_ITC.1** verhindert Angriffe durch Manipulationen der übertragenen Informationen.

Z.SysAdmin

Die Evaluationsstufe **EAL4** gewährleistet ein ausreichendes Vertrauen in die Zuverlässigkeit des EVG. Hierzu gehört auch die Möglichkeit der Verwaltung des EVG durch entsprechend befugtes Personal.

Die Möglichkeit zur Verwaltung des Systems wird durch die ausgewählten Komponenten der Klasse FMT – Sicherheitsmanagement – , d.h. **FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2** und **FMT_SMR.3** bereitgestellt. Diese Komponenten schränken Managementaktivitäten zudem teilweise auf die identifizierte Rolle des Systemverwalters ein.

Der Systemverwalter ist nach **FAU_SEL.1** in der Lage, die Sicherheitsprotokollierung zu verwalten, in dem er bestimmt, welche Ereignisse protokolliert werden sollen und welche von der Protokollierung auszuschließen sind.

Werden kryptographische Verfahren zum Betrieb des EVG eingesetzt, so stehen dem Systemverwalter nach **FCS_CKM.1, FCS_CKM.2, FCS_CKM.3** und **FCS_CKM.4** Verfahren zu Erzeugung, Verteilung, Zugriff und Vernichtung von kryptographischen Schlüsseln zur Verfügung.

Z.Betrieb

Durch die Auswahl der Evaluationsstufe **EAL4** wird dem EVG bereits ein ausreichendes Vertrauen in die Zuverlässigkeit bezüglich der korrekten Funktionsweise und deren Aufrechterhaltung entgegengebracht. **ADV_INT.1** und **ALC_FLR.3** stellen sicher, daß alle Schnittstellen zwischen Modulen des EVG ausreichend beschrieben sind und gemeldete Fehler vom Hersteller systematisch behoben werden.

Die Komponente **FPT_RVM.1** stellt die Unumgehbarkeit aller Sicherheitsfunktionen des EVG sicher.

Durch **FPT_PHP.3** wird gewährleistet, daß die korrekte Funktionsweise der Sicherheitsfunktionen des EVG auch nach materiellen Angriffen ge-

gen den EVG nicht gefährdet ist.

Die Bereichsseparierung nach Komponente **FPT_SEP.2** gewährleistet den Schutz der Sicherheitsfunktionen des EVG vor Eingriffen und Manipulationen durch nicht vertrauenswürdige Subjekte.

Bei Erstanlauf des EVG stellen die Anforderungen der Komponenten **FPT_AMT.1** und **FPT_TST.1** sicher, daß der EVG Selbsttests durchführt und damit verifiziert, daß er sich in einem sicheren Ausgangszustand befindet.

Nach **FPT_FLS.1** wird ein sicherer Zustand des EVG nach Auftreten von Fehlern eingenommen. Diensteunterbrechungen führen ebenfalls nach **FPT_RCV.1** zu einem Übergang des EVG in einen Wartungszustand, aus dem der EVG in einen sicheren Zustand zurückversetzt werden kann.

Der Export von TSF-Daten wird durch die Anforderungen der Komponenten **FPT_ITA.1, FPT_ITC.1** und **FPT_ITI.1** bezüglich Integrität, Verfügbarkeit und Vertraulichkeit überwacht und kann somit zu keiner unsicheren Funktionsweise des EVG führen.

Durch Bereitstellung mehrfacher Authentisierungsmechanismen nach **FIA_UAU.5** können die sensiblen Funktionsbereiche des EVG durch starke Authentisierungsmechanismen besonders geschützt werden.

Die Integrität der Benutzerdaten wird nach **FDP_SDI.2** überwacht, und Zugriffe und nicht integere Daten werden vom EVG unterbunden.

Das Management der Sicherheitsfunktionen des EVG wird durch die Komponenten **FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3** und **FMT_MTD.2** spezifiziert. Insbesondere werden solche Aktivitäten, die die Funktionsweise des EVG beeinträchtigen können, auf autorisierte Rollen eingeschränkt, die ein besonderes Maß an Vertrauenswürdigkeit genießen.

Z.Status

Die Komponenten **FPT_AMT.1** und **FPT_TST.1** stellen sicher, daß dem Systemverwalter bei Erstanlauf und auf Anforderung die Ergebnisse der internen Selbsttests in Form eines Statusreports zur Verfügung gestellt werden.

Potentielle Verletzungen der Sicherheit der Funktionen des EVG werden dem Systemverwalter aufgrund der Komponenten **FAU_SAA.1** und **FAU_ARP.1** mitgeteilt.

Die Komponenten **FAU_SAR.1** und **FAU_SAR.3** stellen sicher, daß der Systemverwalter die Protokollaufzeichnungen lesen und werkzeugunterstützt bezüglich möglicherweise oder tatsächlich stattgefundener Sicherheitsverletzungen durchsehen kann.

Durch die von **FTA_TAH.1** sichergestellte Anzeige des Zeitpunktes der letzten Anmeldung kann der Systemverwalter verifizieren, ob in der Zwischenzeit Angriffe auf die Benutzerkennung des Systemverwalter stattgefunden haben und eventuell erfolgreich gewesen sind.

Die Möglichkeit zur Einsicht in Protokollierungsdateien und Veränderung von diesbezüglichen Sicherheitsattributen wird durch **FMT_MTD.1** und **FMT_MTD.2** auf die vom Systemverwalter einnehmbare Rolle des Audi-

tors beschränkt.

Z.Zustand

Die Evaluationsstufe **EAL4** bestätigt bereits ein ausreichendes Vertrauen in den EVG, einen sicheren Zustand auch im Fehlerfall beizubehalten. Dieser Zustand kann nach **FPT_PHP.3** auch durch materielle Angriffe auf den EVG nicht beeinflußt werden.

Nach **FPT_FLS.1** wird ein sicherer Zustand des EVG nach Auftreten von Fehlern eingenommen.

Bei Erstanlauf wird der sichere Zustand des EVG durch die Tests nach **FPT_AMT.1** und **FPT_TST.1** verifiziert.

Die Integrität der Benutzerdaten wird nach **FDP_SDI.2** überwacht. Zugriffe auf nicht integere Daten werden vom EVG unterbunden, so daß auf diese Weise kein unsicherer Zustand entstehen kann.

Unsichere Zustände durch Überlauf der Protokollierungsdatei werden durch die Anforderung der Komponente **FAU_STG.4** verhindert.

Z.Verbindung

Durch Bereitstellung eines vertrauenswürdigen Pfades und eines vertrauenswürdigen Kanals durch die Anforderungen der Komponenten **FTP_TRP.1** und **FTP_ITC.1** können vertrauenswürdige Verbindungen zwischen Komponenten und Benutzern des EVG einerseits und anderen Komponenten des EVG andererseits aufgebaut werden.

Die Erhaltung der Verfügbarkeit, der Vertraulichkeit und der Integrität von übertragenen Informationen wird durch die ausgewählten Komponenten **FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FDP_UCT.1** und **FDP_UIT.1** gewährleistet.

Durch Verwendung von kryptographischen Verfahren nach **FCS_COP.1** und Einsatz kryptographischer Schlüssel nach **FCS_CKM.3** und **FCS_CKM.4** für die Dauer einer Verbindung zwischen vertrauenswürdigen Komponenten über nicht vertrauenswürdige Verbindungsleitungen können die übertragenen Daten dennoch vor dem Verlust der Vertraulichkeit und Integrität geschützt werden. Die Lebensdauer verwendeter Schlüssel kann mit **FMT_SAE.1** verwaltet werden.

Die Zugriffskontrollpolitiken der Komponente **FDP_ACF.1** können den Zugriff auf gemeinsame Daten im Verlauf einer Kommunikation in Abhängigkeit von den Sicherheitsattributen beider Kommunikationspartner einschränken.

Die Komponenten **FIA_UAU.4** und **FIA_UAU.5** stellen sicher, daß sich beide Kommunikationspartner angemessen authentisieren und im Falle einer starken Authentisierung eine Wiederverwendung von Authentisierungsdaten für weitere Kommunikationen unterbunden wird. Zudem wird durch **FPT_RPL.1** die Wiedereinspielung von Informationen erkannt und abgewehrt. Kommt es im Verlauf der Authentisierung zu Fehlern, wird auf diese vom EVG gemäß **FIA_AFL.1** angemessen reagiert.

Die Nichtumgehbarkeit der Sicherheitsfunktionen des EVG nach **FPT_RVM.1** und die Bereichsseparierung der Sicherheitsfunktionen des EVG nach **FPT_SEP.2** stellen sicher, daß durch bestehende Verbindungen zu externen Kommunikationspartnern die Sicherheitsrichtlinien nicht verletzt oder umgangen werden können.

Z.Verfügbarkeit

Die Anforderungen der Komponente **FPT_ITA.1** gewährleisten die Ver-

fügbarkeit der sicherheitsrelevanten Daten.

Z.Software Dieses Sicherheitsziel wird durch die Anforderungen an die Vertrauenswürdigkeit nach **EAL4** und **ADV_INT.1** und **ALC_FLR.3** ausreichend abgedeckt.

8.3.1.2 Sicherheitsziele für die Umgebung

Die Sicherheitsziele für die Umgebung des EVG sind grundsätzlich durch die Umgebung und nicht durch Funktionalitäten des EVG abzudecken. Dennoch sind einige Anforderungen an die Funktion und die Vertrauenswürdigkeit des EVG durchaus geeignet, zur Abdeckung dieser Sicherheitsziele beizutragen. Diese Anforderungen sind im folgenden aufgeführt.

Z.Installation Durch die Komponenten **FPT_AMT.1** und **FPT_TST.1** wird sichergestellt, daß bei Erstanlauf des EVG nach erfolgter Installation sowie auf Anforderung durch einen befugten Benutzer jeweils Tests der abstrakten Maschine und der Sicherheitsfunktionen durchgeführt werden, deren Ergebnisse als Nachweis für die korrekte Installation des EVG dienen.

Z.Definition Die Definition von Rollen wird durch die rollenbasierte Zugriffskontrollpolitik der Komponenten **FDP_ACC.1** und **FDP_ACF.1** unterstützt.

Der EVG ist in der Lage, unter Anwendung der Komponente **FTA_LSA.1** die Annahme einer Rolle durch einen Benutzer parametrisierbar einzuschränken.

Z.Geheim Die Anforderungen von **FIA_UAU.7** garantieren, daß die von Benutzern eingegebenen Authentisierungsgeheimnisse während der Eingabe nicht angezeigt werden.

Z.Schutz Die Widerstandsfähigkeit des EVG gegen materielle Angriffe nach **FPT_PHP.3** unterstützt die Umsetzung des Sicherheitsziels für die Umgebung, da selbst bei Ausfall sonstiger umgebungsspezifischer Sicherheitsmaßnahmen der EVG durch materielle Angriffe nicht in seiner Sicherheitsfunktion beeinträchtigt werden kann.

8.3.2 Abdeckung der Sicherheitsziele durch die Sicherheitsfunktionen

Die nachfolgende Tabelle zeigt, welche Sicherheitsziele für den EVG und für die Umgebung durch welche Sicherheitsanforderungen der CC abgedeckt werden.

Dabei ist zu beachten, daß die Sicherheitsziele für die Umgebung grundsätzlich von der Umgebung abzudecken sind und die in nachfolgender Tabelle für diese Sicherheitsziele aufgeführten Komponenten diese nicht vollständig abdecken können. Die Komponenten werden vielmehr aus rein informativen Gründen mit aufgeführt, um die Mitwirkung der Sicherheitsanforderungen für den EVG an der Abdeckung der Sicherheitsziele für die Umgebung aufzuzeigen.

Sicherheitsziel	Sicherheitsanforderung
Sicherheitsziele für den EVG	
Z.Zugang	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2, FMT_MSA.3, FMT_REV.1, FMT_SAE.1,

Sicherheitsziel	Sicherheitsanforderung
	FPT_PHP.3, FPT_RPL.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2, FTA_TSE.1, FTP_TRP.1
Z.Zugriff	FAU_SAR.2, FAU_STG.2, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_RIP.2, FDP_UCT.1, FDP_UIT.1, FIA_ATD.1, FIA_UAU.6, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1,FMT_MTD.2, FMT_REV.1, FMT_SMR.1, FMT_SMR.2, FPT_PHP.3, FPT_RPL.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2
Z.Archiv	FDP_SDI.2, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RCV.1, FDP_UCT.1, FDP_UIT.1
Z.Verantwortung	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2, FAU_STG.4, FCO_NRO.1, FCO_NRR.1, FDP_ACC.1, FDP_ACF.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MTD.1, FMT_MTD.2, FMT_SMR.3, FPT_RPL.1, FPT_STM.1, FTA_MCS.1, FTA_TAH.1
Z.Zeit-Ort	FIA_ATD.1, FMT_SAE.1, FPT_STM.1, FTA_LSA.1, FTA_TSE.1
Z.Schutz	FPT_PHP.3
Z.Umgehung	EAL4, FAU_STG.2, FAU_STG.4, FIA_AFL.1, FIA_UAU.4, FPT_ITI.1, FPT_PHP.3, FPT_RPL.1, FPT_RVM.1, FPT_SEP.2, FTP_ITC.1, FTP_TRP.1, FTP_ITC.1
Z.Fehler	ADV_INT.1, ALC_FLR.3, EAL4, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.5, FMT_MSA.2, FMT_SAE.1, FPT_ITC.1, FTA_SSL.1
Z.SysAdmin	EAL4, FAU_SEL.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3
Z.Betrieb	ADV_INT.1, ALC_FLR.3, EAL4, FDP_SDI.2, FIA_UAU.5, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.2, FPT_PHP.3, FPT_AMT.1, FPT_FLS.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FPT_RCV.1, FPT_RVM.1, FPT_SEP.2, FPT_TST.1
Z.Status	FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3,

Sicherheitsziel	Sicherheitsanforderung
	FMT_MTD.1, FMT_MTD.2, FPT_AMT.1, FPT_TST.1, FTA_TAH.1
Z.Verbindung	FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FIA_AFL.1, FIA_UAU.4, FIA_UAU.5, FMT_SAE.1, FPT_ITA.1, FPT_ITI.1, FPT_ITC.1, FPT_RPL.1, FPT_RVM.1, FPT_SEP.2, FTP_ITC.1, FTP_TRP.1
Z.Verfügbarkeit	FPT_ITA.1
Z.Zustand	EAL4, FAU_STG.4, FDP_SDI.2, FPT_AMT.1, FPT_FLS.1, FPT_PHP.3, FPT_TST.1
Z.Software	ADV_INT.1, ALC_FLR.3, EAL4
Sicherheitsziele für die Umgebung	
Z.Installation	FPT_AMT.1, FPT_TST.1
Z.Definition	FDP_ACC.1, FDP_ACF.1, FTA_LSA.1
Z.Geheim	FIA_UAU.7

Tabelle 12: Abdeckung der Sicherheitsziele des EVG durch die Sicherheitsanforderungen der CC

Die nachfolgende Tabelle ist die Umkehrabbildung von Tabelle 12 und zeigt, welche funktionalen Komponenten der CC die einzelnen Sicherheitsziele des EVG abdecken. Der Tabelle ist zu entnehmen, daß jede funktionale Komponenten mindestens ein Sicherheitsziel des EVG abdeckt.

Nr.	Funktion	Sicherheitsziel
FIA – Identifikation und Authentisierung		
1	FIA_UID.2	Z.Verantwortung, Z.Zugang, Z.Zugriff
2	FIA_USB.1	Z.Verantwortung, Z.Zugriff
3	FIA_ATD.1	Z.Zeit-Ort, Z.Zugang, Z.Zugriff
4	FIA_UAU.2	Z.Zugang
5	FIA_UAU.4	Z.Umgehung, Z.Verantwortung, Z.Verbindung, Z.Zugang
6	FIA_UAU.5	Z.Betrieb, Z.Fehler, Z.Verantwortung, Z.Verbindung, Z.Zugang
7	FIA_UAU.6	Z.Verantwortung, Z.Zugang, Z.Zugriff
8	FIA_UAU.7	Z.Geheim, Z.Verantwortung, Z.Zugang
9	FIA_SOS.1	Z.Fehler, Z.Verantwortung, Z.Zugang
10	FIA_AFL.1	Z.Fehler, Z.Umgehung, Z.Verbindung, Z.Zugang
FTA – EVG-Zugriff		

Nr.	Funktion	Sicherheitsziel
11	FTA_TSE.1	Z.Zugang, Z.Zeit-Ort
12	FTA_LSA.1	Z.Definition, Z.Zeit-Ort
13	FTA_SSL.1	Z.Fehler, Z.Zugang, Z.Zugriff
14	FTA_SSL.2	Z.Zugang, Z.Zugriff
15	FTA_MCS.1	Z.Verantwortung, Z.Zugang, Z.Zugriff
16	FTA_TAH.1	Z.Verantwortung, Z.Status
FDP – Schutz der Benutzerdaten		
17	FDP_ACC.1	Z.Verantwortung, Z.Zugriff, Z.Definition
18	FDP_ACF.1	Z.Verantwortung, Z.Zugriff, Z.Verbindung, Z.Definition
19	FDP_SDI.2	Z.Betrieb, Z.Zustand, Z.Archiv
20	FDP_UCT.1	Z.Zugriff, Z.Verbindung, Z.Archiv
21	FDP_UIT.1	Z.Verbindung, Z.Zugriff, Z.Archiv
22	FDP_RIP.2	Z.Zugriff
FPT – Schutz der EVG-Sicherheitsfunktionen		
23	FPT_PHP.3	Z.Schutz, Z.Umgehung, Z.Zugang, Z.Zugriff, Z.Zustand, Z.Betrieb
24	FPT_RVM.1	Z.Betrieb, Z.Umgehung, Z.Verbindung
25	FPT_SEP.2	Z.Betrieb, Z.Umgehung, Z.Verbindung
26	FPT_AMT.1	Z.Betrieb, Z.Installation, Z.Status, Z.Zustand
27	FPT_TST.1	Z.Betrieb, Z.Installation, Z.Status, Z.Zustand
28	FPT_FLS.1	Z.Betrieb, Z.Zustand
29	FPT_RCV.1	Z.Archiv, Z.Betrieb
30	FPT_ITA.1	Z.Betrieb, Z.Verbindung, Z.Verfügbarkeit, Z.Archiv
31	FPT_ITC.1	Z.Betrieb, Z.Fehler, Z.Umgehung, Z.Verbindung, Z.Archiv
32	FPT_ITI.1	Z.Betrieb, Z.Umgehung, Z.Verbindung, Z.Archiv
33	FPT_RPL.1	Z.Umgehung, Z.Verantwortung, Z.Verbindung, Z.Zugang, Z.Zugriff
34	FPT_STM.1	Z.Verantwortung, Z.Zeit-Ort
FCO – Kommunikation		
35	FCO_NRO.1	Z.Verantwortung
36	FCO_NRR.1	Z.Verantwortung
FTP – Vertrauenswürdiger Pfad/Kanal		

Nr.	Funktion	Sicherheitsziel
37	FTP_TRP.1	Z.Umgehung, Z.Zugang, Z.Verbindung
38	FTP_ITC.1	Z.Umgehung, Z.Verbindung
FCS – Kryptographische Unterstützung		
39	FCS_COP.1	Z.Fehler, Z.Verbindung, Z.Zugriff
40	FCS_CKM.1	Z.Fehler, Z.SysAdmin, Z.Zugriff
41	FCS_CKM.2	Z.Fehler, Z.SysAdmin, Z.Zugriff,
42	FCS_CKM.3	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zugriff
43	FCS_CKM.4	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zugriff
FAU – Sicherheitsprotokollierung		
44	FAU_GEN.1	Z.Verantwortung
45	FAU_GEN.2	Z.Verantwortung
46	FAU_SEL.1	Z.SysAdmin, Z.Verantwortung
47	FAU_SAA.1	Z.Status, Z.Verantwortung
48	FAU_ARP.1	Z.Status, Z.Verantwortung
49	FAU_STG.2	Z.Umgehung, Z.Verantwortung, Z.Zugriff
50	FAU_STG.4	Z.Umgehung, Z.Verantwortung, Z.Zustand
51	FAU_SAR.1	Z.Status, Z.Verantwortung
52	FAU_SAR.2	Z.Zugriff
53	FAU_SAR.3	Z.Status, Z.Verantwortung
FMT – Sicherheitsmanagement		
54	FMT_MOF.1	Z.Betrieb, Z.SysAdmin, Z.Zugriff
55	FMT_MSA.1	Z.Betrieb, Z.SysAdmin, Z.Zugriff
56	FMT_MSA.2	Z.Betrieb, Z.Fehler, Z.SysAdmin
57	FMT_MSA.3	Z.Betrieb, Z.SysAdmin, Z.Zugang, Z.Zugriff
58	FMT_MTD.1	Z.Status, Z.SysAdmin, Z.Verantwortung., Z.Zugriff
59	FMT_MTD.2	Z.Betrieb, Z.Status, Z.SysAdmin, Z.Verantwortung, Z.Zugriff
60	FMT_REV.1	Z.SysAdmin, Z.Zugang, Z.Zugriff
61	FMT_SAE.1	Z.Fehler, Z.SysAdmin, Z.Verbindung, Z.Zeit-Ort, Z.Zugang
62	FMT_SMR.1	Z.SysAdmin, Z.Zugriff
63	FMT_SMR.2	Z.SysAdmin, Z.Zugriff
64	FMT_SMR.3	Z.SysAdmin, Z.Verantwortung

Tabelle 13: Beitrag der funktionalen Komponenten der CC zu den Sicherheitszielen des EVG

Die nachfolgende Tabelle zeigt, daß die in den ausgewählten funktionalen Komponenten enthaltenen Abhängigkeiten berücksichtigt sind, indem

- die abhängige Komponente direkt in der Liste der funktionalen Komponenten vorhanden ist, oder eine hierarchisch höherstehende Komponente ausgewählt wurde, die die geforderte Komponente vollständig enthält.
- bei alternativ auszuwählenden Komponenten eine der alternativen Komponenten ausgewählt wurde.

Nr.	Komponente	Abhängigkeiten	Abgedeckt durch	Referenz-Nr.
1	FIA_UID.2	—		
2	FIA_USB.1	FIA_ATD.1	FIA_ATD.1	3
3	FIA_ATD.1	—		
4	FIA_UAU.2	FIA_UID.1	FIA_UID.2	1(H)
5	FIA_UAU.4	—		
6	FIA_UAU.5	—		
7	FIA_UAU.6	—		
8	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	4(H)
9	FIA_SOS.1	—		
10	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	4(H)
11	FTA_TSE.1	—		
12	FTA_LSA.1	—		
13	FTA_SSL.1	FIA_UAU.1	FIA_UAU.2	4(H)
14	FTA_SSL.2	FIA_UAU.1	FIA_UAU.2	4(H)
15	FTA_MCS.1	FIA_UID.1	FIA_UID.2	1(H)
16	FTA_TAH.1	—		
17	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	18
18	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	17
		FMT_MSA.3	FMT_MSA.3	57
19	FDP_SDI.2	—		
20	FDP_UCT.1	FDP_ACC.1 FDP_IFC.1	FDP_ACC.1	17
		FTP_ITC.1 FTP_TRP.1	FTP_ITC.1 FTP_TRP.1	38 37
21	FDP_UIT.1	FDP_ACC.1 FDP_IFC.1	FDP_ACC.1	17
		FTP_ITC.1 FTP_TRP.1	FTP_ITC.1 FTP_TRP.1	38 37

Nr.	Komponente	Abhängigkeiten	Abgedeckt durch	Referenz-Nr.
22	FDP_RIP.2	—		
23	FPT_PHP.3	—		
24	FPT_RVM.1	—		
25	FPT_SEP.2	—		
26	FPT_AMT.1	—		
27	FPT_TST.1	FPT_AMT.1	FPT_AMT.1	26
28	FPT_FLS.1	ADV_SPM.1	ADV_SPM.1	EAL4
29	FPT_RCV.1	FPT_TST.1	FPT_TST.1	27
		AGD_ADM.1	AGD_ADM.1	EAL4
		ADV_SPM.1	ADV_SPM.1	EAL4
30	FPT_ITA.1	—		
31	FPT_ITC.1	—		
32	FPT_ITI.1	—		
33	FPT_RPL.1	—		
34	FPT_STM.1	—		
35	FCO_NRO.1	FIA_UID.1	FIA_UID.2	1(H)
36	FCO_NRR.1	FIA_UID.1	FIA_UID.2	1(H)
37	FTP_TRP.1	—		
38	FTP_ITC.1	—		
39	FCS_COP.1	FDP_ITC.1 FCS_CKM.1	FCS_CKM.1	40
		FCS_CKM.4	FCS_CKM.4	43
		FMT_MSA.2	FMT_MSA.2	56
40	FCS_CKM.1	FCS_CKM.2 FCS_COP.1	FCS_CKM.2	41
		FCS_CKM.4	FCS_CKM.4	43
		FMT_MSA.2	FMT_MSA.2	56
41	FCS_CKM.2	FDP_ITC.1 FCS_CKM.1	FCS_CKM.1	40
		FCS_CKM.4	FCS_CKM.4	43
		FMT_MSA.2	FMT_MSA.2	56
42	FCS_CKM.3	FDP_ITC.1 FCS_CKM.1	FCS_CKM.1	40
		FCS_CKM.4	FCS_CKM.4	43

Nr.	Komponente	Abhängigkeiten	Abgedeckt durch	Referenz-Nr.
		FMT_MSA.2	FMT_MSA.2	56
43	FCS_CKM.4	FDP_ITC.1 FCS_CKM.1	FCS_CKM.1	40
		FMT_MSA.2	FMT_MSA.2	56
44	FAU_GEN.1	FPT_STM.1	FPT_STM.1	34
45	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	44
		FIA_UID.1	FIA_UID.2	1(H)
46	FAU_SEL.1	FAU_GEN.1	FAU_GEN.1	44
		FMT_MTD.1	FMT_MTD.1	58
47	FAU_SAA.1	FAU_GEN.1	FAU_GEN.1	44
48	FAU_ARP.1	FAU_SAA.1	FAU_SAA.1	47
49	FAU_STG.2	FAU_GEN.1	FAU_GEN.1	44
		FAU_GEN.1	FAU_GEN.1	44
50	FAU_STG.4	FAU_STG.1	FAU_STG.2	49(H)
51	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	44
52	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	51
53	FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	51
54	FMT_MOF.1	FMT_SMR.1	FMT_SMR.1	62
55	FMT_MSA.1	FDP_ACC.1 FDP_IFC.1	FDP_ACC.1	17
		FMT_SMR.1	FMT_SMR.1	62
56	FMT_MSA.2	ADV_SPM.1	ADV_SPM.1	EAL4
		FDP_ACC.1 FDP_IFC.1	FDP_ACC.1	17
		FMT_MSA.1	FMT_MSA.1	55
		FMT_SMR.1	FMT_SMR.1	62
57	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	55
		FMT_SMR.1	FMT_SMR.1	62
58	FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	62
59	FMT_MTD.2	FMT_MTD.1	FMT_MTD.1	58
		FMT_SMR.1	FMT_SMR.1	62
60	FMT_REV.1	FMT_SMR.1	FMT_SMR.1	62
61	FMT_SAE.1	FMT_SMR.1	FMT_SMR.1	62
		FPT_STM.1	FPT_STM.1	34

Nr.	Komponente	Abhängigkeiten	Abgedeckt durch	Referenz-Nr.
62	FMT_SMR.1	FIA_UID.1	FIA_UID.2	1(H)
63	FMT_SMR.2	FIA_UID.1	FIA_UID.2	1(H)
64	FMT_SMR.3	FMT_SMR.1	FMT_SMR.1	62

Tabelle 14: Abdeckung der funktionalen Abhängigkeiten

8.4 Erklärung zur Auswahl der Anforderungen an die Vertrauenswürdigkeit

8.4.1 Vertrauenswürdigkeitsstufe 4 (EAL4) – methodisch entwickelt, getestet und durchgesehen

Die Anforderungen des Schutzprofils SIZ-PP an die Vertrauenswürdigkeit gründen sich im wesentlichen auf die Vertrauensbeziehungen, die üblicherweise zwischen Kunden und Finanzdienstleistern bestehen. Die finanziellen Werte, die die Kunden ihrem Bankinstitut im Rahmen von Geschäftsvorfällen anvertrauen, existieren mehrheitlich nur noch in elektronischer Form innerhalb der IT-Systeme, weshalb der Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der IT-Systeme und der mit ihnen verarbeiteten Informationen direkt die materielle Existenz vieler Kunden bedrohen würde und einen umfassenden Vertrauensverlust in das Bankinstitut nach sich ziehen könnte. Damit hängt auch die wirtschaftliche Existenz des Bankinstituts unmittelbar von der IT-Sicherheit seiner IT-Systeme ab. Neben den erforderlichen Sicherheitsfunktionen müssen die eingesetzten IT-Systeme ein Maß an Vertrauenswürdigkeit erreichen, das geeignet ist, das Vertrauen der Kunden in das Bankinstitut zu rechtfertigen. Das gemeinsame Sicherheitsbedürfnis der Institute und Kunden erfordert daher die Wahl einer möglichst hohen Vertrauenswürdigkeitsstufe.

Auf der anderen Seite stehen dem das Problem der außerordentlichen Komplexität der eingesetzten IT-Systeme entgegen, die sich aus der Vielfalt der Bankgeschäfte und der zunehmenden Vernetzung der IT-Systeme ergibt. Diese Komplexität begrenzt die erreichbare Vertrauenswürdigkeit des IT-Gesamtsystems nach oben.

Unter Berücksichtigung der Sicherheitsbedürfnisses einerseits und der Systemkomplexität andererseits erscheint EAL4 als höchste erreichbare Stufe der Vertrauenswürdigkeit. Sie steht auch im Einklang mit den Anforderungen des SIZ-Anwendungsentwicklungsmodells (SIZ-AE-Modell), das vergleichbare Maßnahmen für die Entwicklung von Software in der SKO fordert.

ADV_INT.1 Modularität

Diese Erweiterung adressiert die Komplexität der bei den Finanzdienstleistern zum Einsatz kommenden IT-Systeme. Solche IT-Systeme bestehen üblicherweise aus einer Reihe von Hard- und Softwarekomponenten, die von grundlegenden Betriebssystemfunktionen bis hin zu spezialisierten bankfachlichen Anwendungen reichen. Die Komponenten können von mehreren Herstellern entwickelt und bereitgestellt werden. Um die

Gesamtheit der erforderlichen Dienste für die Benutzer zur Verfügung stellen zu können, müssen die Komponenten miteinander interagieren. Nur durch die Modularität im Sinne von ADV_INT.1 kann die dadurch entstehende Komplexität beherrscht werden.

ADV_INT.1 hat folgende Abhängigkeiten:

ADV_IMP.1 – Teilmenge der Implementierung der TSF

ADV_LLD.1 – Beschreibender Entwurf auf niedriger Ebene

Diese Abhängigkeiten werden durch die in EAL4 enthaltenen Anforderungen zur Vertrauenswürdigkeit abgedeckt.

ALC_FLR.3 – Systematische Fehlerbehebung

Die Komplexität der zum Einsatz kommenden IT-Systeme kann selbst bei einer Entwicklung nach den in EAL4 vorgegebenen Anforderungen nicht ausschließen, daß Fehler in einzelnen Komponenten entdeckt werden, die die IT-Sicherheit gefährden können. Im Interesse der Kunden und Anwender müssen solche Fehler schnell und zuverlässig gemeldet und behoben werden können, um die Ausnutzung erkannter Fehler und die damit verbundenen möglicherweise erheblichen Schäden zu vermeiden. Eine systematische Fehlerbehebung im Sinne von ALC_FLR.3 zur Absicherung der Interessen der Institute und ihrer Kunden ist daher zwingend erforderlich.

Die Komponente hat keine Abhängigkeiten, die durch andere Anforderungen abzudecken wären.

8.5 Konsistenz der Sicherheitsanforderungen

Dieser Abschnitt der Erklärungen weist nach, daß die Menge der ausgewählten IT-Sicherheitsanforderungen ein sich gegenseitig unterstützendes und in sich geschlossenes Ganzes bildet.

Die Sicherheitsanforderungen wurden auf der Basis des IT-Sicherheitsstandards des SIZ gewonnen, der die Anforderungen der Mitglieder der Sparkassenorganisation bezüglich der Sicherheit ihrer IT-Systeme beschreibt und die Erfahrungen der SKO-Mitglieder zusammenfaßt. Diese im langjährigen Umgang mit IT-Sicherheit und der Erfüllung gesetzlicher Anforderungen an die IT-Sicherheit in den Instituten gewonnenen Erfahrungen gewährleisten für sich ein konsistentes und in sich geschlossenes Ganzes der Sicherheitsanforderungen.

Nach der Übertragung der Anforderungen in die Struktur des vorliegenden Schutzprofils wurde in den hier vorliegenden Erklärungen gezeigt, daß die funktionalen Anforderungen in sich konsistent sind, da alle Abhängigkeiten der funktionalen Anforderungen untereinander und die Abhängigkeiten zwischen funktionalen Anforderungen und den Anforderungen zur Vertrauenswürdigkeit erfüllt sind (vgl. Tabelle 14).

Aus den Anforderungen an die Vertrauenswürdigkeit wurde mit der Vertrauenswürdigkeitsstufe EAL4 eine geprüfte und allgemein akzeptierte Kombination in sich konsistenter Anforderungen gewählt. In Abschnitt 8.4 wurde zudem gezeigt, daß die ausgewählten Erweiterungen erforderlich und mit den bestehenden Anforderungen konsistent sind.