Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0007-2002

zu

Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU), Version 2.01

entwickelt vom

Bundesbeauftragten für den Datenschutz

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

Bundesamt für Sicherheit in der Informationstechnik

Zertifikat BSI-PP-0007-2002

Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU), Version 2.01

Common Criteria Vereinbarung

entwickelt vom

Bundesbeauftragten für den Datenschutz

Vertrauenswürdigkeitspaket: **EAL 2** mit Zusatz

Bonn, den 27. September 2002

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Henze L.S.

Das oben genannte Schutzprofil wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.0,* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Teil 1 Version 0.6, Teil 2 Version 1.0*, evaluiert.

Dieses Zertifikat gilt nur für die angegebene Version des Schutzprofils und nur in Verbindung mit dem vollständigen Zertifizierungsreport.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlußfolgerungen der Prüfstelle stehen in Einklang mit den erbrachten Nachweisen.

Mit diesem Zertifikat ist weder eine generelle Empfehlung des Schutzprofils noch eine Garantie des Bundesamtes für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte, verbunden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] neben der Zertifizierung von Sicherheitsprodukten der Informationstechnik auch die Aufgabe, Schutzprofile (PP)[2] für solche Produkte zu zertifizieren.

Ein Schutzprofil definiert eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen an eine Kategorie von Produkten (Systeme oder Komponenten). Anwender können durch Erstellung und Zertifizierung eines Schutzprofils oder Verweis auf ein solches ihre IT-Sicherheitsbedürfnisse ausdrücken, ohne Bezug auf ein konkretes Produkt zu nehmen. Schutzprofile können als Grundlage für eine Produktzertifizierung herangezogen werden. Produkte, die eine solche Zertifizierung durchlaufen haben, erhalten ein eigenes Zertifikat.

Die Zertifizierung eines Schutzprofils wird auf Veranlassung des Schutzprofil-Entwicklers - im folgenden Antragsteller genannt - durchgeführt. Entwickler eines Schutzprofils können IT-Hersteller, aber auch IT-Anwender sein.

Bestandteil des Verfahrens ist die Evaluierung (Prüfung und Bewertung) des Schutzprofils gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Evaluierung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder von der Prüfstelle des BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Schutzprofils, die Einzelheiten der Bewertung und Hinweise für den Anwender.

---

1 Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

2 Protection Profile

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSIG[3]
- BSI-Zertifizierungsverordnung[4]
- BSI-Kostenverordnung[5]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung [BSI 7125]
- Vorläufiges Verfahren der Erteilung eines PP-Zertifikats durch das BSI
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik [CC], Version 2.1[6] (ISO/IEC 15408)
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik [CEM]
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0
- BSI Zertifikate: Anwendungshinweise und Interpretationen zum Schema [AIS]

---

[3] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

[4] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7.Juli 1992, Bundesgesetzblatt I S. 1230

[5] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 29. Oktober 1992, Bundesgesetzblatt I S. 1838

[6] Bekanntmachung des Bundesministeriums des Innern vom 22. September 2000

2 Anerkennungsvereinbarungen

Um die Mehrfach-Entwicklung des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von Zertifikaten für Schutzprofile unter gewissen Bedingungen vereinbart.

Im Mai 2000 wurde eine Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Israel trat im November 2000 der Vereinbarung bei und Schweden im Februar 2002.

3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Schutzprofil ´Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU)´, Version 2.01 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils ´Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU)´, Version 2.01 wurde von der Prüfstelle T-Systems ISS GmbH durchgeführt. Die Prüfstelle T-Systems ISS GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF) [7].

Antragsteller ist der Bundesbeauftragte für den Datenschutz.

Entwickelt wurde das Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU), Version 2.01 im Auftrag des BSI unter Veranlassung des Bundesbeauftragten für den Datenschutz. Auftragnehmer war die DFKI GmbH (Deutsches Forschungszentrum für Künstliche Intelligenz).

Die Entwicklung und Evaluierung des Schutzprofils wurde auf der Grundlage der CC Version 2.1 (ISO/IEC 15408), sowie der AIS durchgeführt.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 27. September 2002 vom BSI abgeschlossen.

[7] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-8.

Das Schutzprofil ´Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU)´, Version 2.01 ist in die BSI-Liste der zertifizierten Schutzprofile, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Entwickler[8] des Schutzprofils angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[8] Bundesbeauftragter für den Datenschutz, Friedrich-Ebert-Str.1, 53173 Bonn, siehe auch Internet: http://www.bfd.bund.de

B Zertifizierungsbericht

Gliederung des Zertifizierungsberichtes

1 PP-Übersicht

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

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

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

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

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

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

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

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

- Betriebssysteme,
- Datenbanksysteme oder
- Email-Clients und -Server.

Die hier beschriebene Sicherheitsleistung geht davon aus, dass eine Unterscheidung von Benutzern nicht erforderlich ist. Falls eine Unterscheidung von Benutzern von der IT-Umgebung unterstützt wird und ihre Berücksichtigung angeraten ist, wird die Verwendung eines TOE (EVG) empfohlen, der mit der Mehrbenutzervariante [BISS-MU] des Schutzprofils BSI-PP-0008-2002 konform ist. (Das Schutzprofil Benutzerbestimmbare Informationsflusskontrolle (SU), Zertifizierungskennung BSI-PP-0007-2002 steht hierarchisch unterhalb des Schutzprofils Benutzerbestimmbare Informationsflusskontrolle (MU), Zertifizierungskennung BSI-PP-0008-2002 [BISS-MU]).

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

Art des Produkts

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

IT-Leistungsmerkmale

Der TOE (EVG) stellt sicher, dass Informationsflüsse sowohl innerhalb des IT-Systems als auch aus dem IT-System hinaus (über eine Verbindung zu offenen Netzen, z.B. LAN, WAN, Internet, Email) in Übereinstimmung mit der zugrunde liegenden EVG-Sicherheitspolitik und gemäß der festgelegten Informationsflussregeln stattfinden. Die Informationsflussregeln können aus vorgegebenen rechtlichen, technischen und organisatorischen Regelungen (z.B. verschlüsselte Speicherung, verschlüsselte Übertragung, signierte Übertragung) abgeleitet werden. In Informationsflussregeln kann festgelegt werden, unter welchen Umständen der TOE (EVG) auf welche Art und Weise mit Daten zu verfahren hat. Die Entscheidung über die Erlaubnis von Informationsflüssen und ihre vorschriftsmäßige Verarbeitung leistet der TOE (EVG) mit Hilfe eines Referenzmonitors, der die Informationsflüsse überwacht.

EVG-Abgrenzung

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

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

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

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

Betriebsumgebung

Es wird angenommen, dass jeder rechtmäßige Benutzer ein Interesse an der Sicherheitsleistung des TOE (EVG) hat und von ihm keine direkten Bedrohungen von Benutzerdaten ausgehen. Um unerwünschte Informationsflüsse, die von rechtmäßigen Benutzern angefordert werden, verhindern zu können, ist eine Unterscheidung der Benutzer nicht notwendig.

Es kann nicht davon ausgegangen werden, dass Administratoren des IT-Systems (insbesondere im Fall einer Fernadministration) in gleichem Umfang wie rechtmäßige Benutzer Interesse an der Sicherheitsleistung des TOE (EVG) haben. Administratoren des IT-Systems werden genauso wie nicht rechtmäßige Benutzer (potentielle Angreifer) als Urheber von Bedrohungen betrachtet. Es wird von einem Angriffspotential ausgegangen, das auf die Fähigkeit zur Durchführung offensichtlicher Penetrationsangriffe beschränkt ist.

Eine Sonderstellung nimmt der EVG-Administrator ein. Er wird ohne Einschränkung als vertrauenswürdig angesehen. Maßnahmen zur Kontrolle der Tätigkeit des EVG-Administrators sind daher nicht vorgesehen.

2 Funktionale Sicherheitsanforderungen

Die folgenden funktionalen Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil verwendet:

Funktionale Sicherheits-anforderung	Beschreibung
FAU_GEN.1	Generierung der Protokolldaten
FAU_SAR.1	Durchsicht der Protokollierung
FAU_SAR.2	Eingeschränkte Durchsicht der Protokollierung
FAU_SAR.3	Auswählbare Durchsicht der Protokollierung
FAU_SEL.1	Auswahl der Ereignisse für die Sicherheitsprotokollierung
FAU_STG.1	Geschützte Speicherung des Protokolls
FAU_STG.3	Aktionen im Fall von möglichem Protokolldaten-Verlust
FDP_ETC.1	Export von Benutzerdaten ohne Sicherheitsattribute
FDP_IFC.1	Teilweise Informationsflusskontrolle
FDP_IFF.1	Einfache Sicherheitsattribute
FDP_ITC.1	Import von Benutzerdaten ohne Sicherheitsattribute
FIA_UAU.1	Zeitpunkt der Authentisierung
FIA_UID.1	Zeitpunkt der Identifikation
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
FMT_MOF.1	Management des Verhaltens der Sicherheitsfunktionen
FMT_MSA.1	Management der Sicherheitsattribute
FMT_MSA.3	Initialisierung statischer Attribute
FMT_MTD.1A	Management der TSF-Daten (*1)
FMT_MTD.1B	
FMT_MTD.3	Sichere TSF-Daten
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Einschränkungen der Sicherheitsrollen
FTA_SSL.3	Durch TSF eingeleitete Beendigung

(*1): FMT_MTD.1A resultiert aus FAU_SEL.1 und
FMT_MTD.1B resultiert aus FMT_MTD.3.

Anforderungen an die IT-Umgebung sind dem Kapitel 5.2 von [BISS-SU] zu entnehmen.

3 Vertrauenswürdigkeitspaket

Die Anforderungen an die Vertrauenswürdigkeit, welche vom TOE (EVG) erfüllt werden müssen, sind in nachfolgender Tabelle aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL 2 aus Teil 3 der Common Criteria erweitert um die Komponente AVA_MSU.3.

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

4 Geforderte Stärke der Funktionen

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil ist:

SoF-mittel.

5 Ergebnis der Evaluierung

Das Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU), Version 2.01 erfüllt die Anforderungen an Schutzprofile, die in den CC in der Klasse APE festgelegt sind.

6 Definitionen

6.1 Abkürzungen

CC Common Criteria, Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

IT Informationstechnik

MU Mehrbenutzervariante

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SoF Strength of Function - Stärke der Funktionen

ST Security Target – Sicherheitsvorgaben

SU Einzelbenutzervariante

EVG Evaluationsgegenstand

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE security policy - EVG-Sicherheitspolitik

6.2 Glossar

Zusatz - Das Hinzufügen einer oder mehrerer Vertrauenswürdigkeitskomponenten aus Teil 3 der CC zu einer EAL oder einem Vertrauenswürdigkeitspaket.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine Einheit im TSC, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Konsumentenbedürfnisse erfüllen.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlaß sein muß.

Sicherheitsvorgaben - Eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Stärke der Funktionen - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

SOF-Niedrig - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

SOF-Mittel - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Hoch - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

Subjekt - Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.

Evaluationsgegenstand - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfaßt, auf die Verlaß sein muß, um die TSP korrekt zu erfüllen.

EVG-Sicherheitspolitik - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

Anwendungsbereich der TSF-Kontrolle - Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können und den Regeln der TSP unterliegen.

7 Literaturangaben

[AIS] Anwendungshinweise und Interpretationen zum Schema (AIS), soweit für den EVG relevant

[BISS-MU] Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Mehrbenutzervariante (MU), Version 2.01, vom 4. September 2002, BSI-PP-0008-2002

[BISS-SU] Schutzprofil Benutzerbestimmbare Informationsflusskontrolle, Einzelbenutzervariante (SU), Version 2.01, vom 4. September 2002, BSI-PP-0007-2002

[CC] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.1 (ISO/IEC 15408)

[CEM] Gemeinsame Methodologie der Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 1 Version 0.6, Teil 2 Version 1.0

[7125] BSI-Zertifizierung: Verfahrensbeschreibung

[7148] BSI-Liste zertifizierter Produkte

Anhang: Schutzprofil