BSI-PP-0001-2000

zu

Schutzprofil
Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, Version 2.0

entwickelt von

Informatikzentrum der Sparkassenorganisation GmbH

Zertifizierungsreport

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Bundesamt für Sicherheit in der Informationstechnik

Zertifikat BSI-PP-0001-2000

Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, Version 2.0

Common Criteria Vereinbarung

entwickelt von

Informatikzentrum der Sparkassenorganisation GmbH

Vertrauenswürdigkeitspaket: **EAL 4**

Bonn, den 25. August 2000

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Henze L.S.

Das oben genannte Schutzprofil wurde von einer 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 183 - 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 2.0[6]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM)
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0

---

[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 16. Februar 1999 im Bundesanzeiger S. 1945

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.

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 Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, Version 2.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, Version 2.0 wurde von der Prüfstelle des BSI durchgeführt.

Antragsteller und Entwickler ist das Informatikzentrum der Sparkassen-organisation GmbH.

Die Zertifizierung erfolgte auf Basis der Common Criteria in der Version 2.0[7]. Die Entwicklung und Evaluierung des Schutzprofils wurde auf der Grundlage der CC Version 2.1 durchgeführt. Die erzielten Ergebnisse sind in vollem Umfang auch für die CC Version 2.0 gültig.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 25. August 2000 vom BSI abgeschlossen.

[7] Bekanntmachung des Bundesministeriums des Innern vom 16. Februar 1999 im Bundes-anzeiger S. 1945

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-7.

Das Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleiter, Version 2.0 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. Internet-adresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[8] SIZ Informatikzentrum der Sparkassenorganisation GmbH, Königswinterer Straße 552, 53227 Bonn

B Zertifizierungsbericht

Gliederung des Zertifizierungsberichtes

1 PP-Übersicht

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 Annahmen finden sich in Abschnitt 4.1.1 „Annahmen zur Betriebsumgebung" 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 beschreibt Anforderungen für eine Umgebung, 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 Funktionale Sicherheitsanforderungen

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

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

Funktionale Sicherheits-anforderung	Bezeichnung
	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 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**
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

Funktionale Sicherheits-anforderung	Bezeichnung
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

3 Vertrauenswürdigkeitspaket

Die folgenden Anforderungen an die Vertrauenswürdigkeit aus Teil 3 der CC werden im vorliegenden Schutzprofil verwendet:

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

4 Geforderte Stärke der Funktionen

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil ist:

SoF-mittel.

5 Ergebnis der Evaluierung

Das Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleiter, Version 2.0 erfüllt die Anforderungen an Schutzprofile, die in den CC in der Klasse APE festgelegt sind.

6 Definitionen

6.1 Abkürzungen

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

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

IT Informationstechnik

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SoF Strength of Function - Stärke der Funktionen

ST Security Target - Sicherheitsvorgaben

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

[CC] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.0

[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

C Schutzprofil