Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-CC-PP-0085-2016

zu

Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0

entwickelt von der

DB Netz AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0085-2016

Common Criteria Schutzprofil

Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA)
Version 1.0

entwickelt durch DB Netz AG

Vertrauenswürdigkeitspaket des Schutzprofiles:
Common Criteria Teil 3 konform
EAL 4 mit Zusatz von
AVA_VAN.5

Gültig bis 10. August 2026

SOGIS Recognition Agreement

Common Criteria

Das in diesem Zertifikat genannte Schutzprofil wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

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.

Common Criteria Recognition Arrangement

Dieses Zertifikat ist keine generelle Empfehlung des Schutzprofils durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das Schutzprofil durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 11. August 2016
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Bernd Kowalski
Abteilungspräsident

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Gliederung

Dies ist eine eingefügte Leerseite.

A Zertifizierung

1 Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG die Aufgabe, neben der Zertifizierung von Produkten der Informationstechnik, auch für Schutzprofile (Protection Profiles, PP) Sicherheitszertifikate zu erteilen.

Ein Schutzprofil definiert eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen an eine Kategorie von Produkten. Anwender oder Bedarfsträger können durch Verwendung 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, aber im Rahmen der Produktevaluierung können die Ergebnisse der PP Zertifizierung bei der Evaluierung der Sicherheitsvorgabe wiederverwendet werden, wenn die Konformität zum Schutzprofil gefordert ist.

Die Zertifizierung eines Schutzprofils geschieht auf Veranlassung des BSI oder eines Bedarfsträgers. Bestandteil des Verfahrens ist die Evaluierung (Prüfung und Bewertung) des Schutzprofils gemäß den Common Criteria [1]. Die Evaluierung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder von der Prüfstelle des BSI durchgeführt. Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

2 Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz (BSIG)[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- BSI-Kostenverordnung[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3], einschließlich PP-Zertifizierung
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]

---

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

2 Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und - Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

3 Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]
- Interne Verfahrensanweisung zur Zertifizierung eines Schutzprofils

3 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart. Daher können die Ergebnisse dieses Evaluierungs- und Zertifizierungsverfahrens im Rahmen einer nachfolgenden Produktevaluierung und -zertifizierung bei der Evaluierung einer Sicherheitsvorgabe wiederverwendet werden.

3.1 Europäische Anerkennung von ITSEC/CC – Zertifikaten (SOGIS-MRA)

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es regelt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe bis einschließlich der Common Criteria (CC) Vertrauenswürdigkeitsstufe EAL4 und ITSEC Vertrauenswürdigkeitsstufen E3 (niedrig) sowie zusätzlich für IT-Produkte aus bestimmten Technischen Bereichen (SOGIS Technical Domains) auf höheren Anerkennungsstufen. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles).

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

Details zur Anerkennung, zu den Technical Domains und zum Abkommen sind unter http://www.sogisportal.eu zu finden.

3.2 Internationale Anerkennung von CC - Zertifikaten

Das internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA) wurde im September 2014 in der derzeit gültigen Fassung ratifiziert. Es deckt CC-Zertifikate für IT-Produkte ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis einschließlich EAL 2 oder der Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren, und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP). In bestimmten Fällen werden Zertifikate, die während einer Übergangszeit bis September 2017 erteilt werden, bis EAL 4 anerkannt.

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

---

[4] Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

Details zur Anerkennung, zu den Technical Communities und zum Abkommen sind unter http://www.commoncriteriaportal.org zu finden.

4 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 Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 wurde von der Prüfstelle SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 04.08.2016 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller für dieses Zertifizierungsverfahren ist: DB Netz AG.

Das Schutzprofil wurde entwickelt von: DB Netz AG.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5 Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Schutzprofils.

Bei Änderungen an der zertifizierten Version des Schutzprofils kann die Gültigkeit auf neue Versionen des Schutzprofils erweitert werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d. h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

Die Bedeutung der CC-Konzepte und -Begriffe ergibt sich aus CC [1] Teil 1 für das PP Konzept, aus CC [1] Teil 2 für die Definition von Funktionalen Sicherheitsanforderungen (SFR) und aus CC [1] Teil 3 für die Definition der Vertrauenswürdigkeitskomponenten, für die Klasse AVA Vulnerability Assessment und die Gegenüberstellung der Vertrauenswürdigkeitsstufen (Evaluation Assurance Levels, EALs) und den Vertrauenswürdigkeitskomponenten.

Die Gültigkeit des Zertifikates endet wie auf dem Zertifikat angegeben. Dem Anwender und dem Auftraggeber für dieses Zertifikat wird empfohlen, den technischen Inhalt des zertifizierten Schutzprofils entsprechend der sich weiterentwickelnden Technologie und der angenommenen operativen Einsatzumgebung des beschriebenen Produkttyps, aber auch hinsichtlich der Weiterentwicklung der Kriterien zu prüfen. Eine solche Überprüfung sollte in einer Aktualisierung und Re-Zertifizierung des Schutzprofils münden. Typischerweise erfolgt eine Überprüfung technischer Standards alle fünf Jahre.

[5] Information Technology Security Evaluation Facility

Die Begrenzung der Gültigkeit dieses Schutzprofil-Zertifikates hat nicht notwendigerweise Einfluss auf die Gültigkeitsdauer eines Produktzertifikates, das dieses Schutzprofil verwendet. Die Zertifizierungsstelle, die ein Produktzertifikat unter Verwendung dieses Schutzprofils erteilt, sollte dies jedoch in die Überlegung zur Gültigkeitsdauer für das Produktzertifikat einbeziehen.

6 Veröffentlichung

Das Schutzprofil Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 ist in die BSI-Liste der zertifizierten Schutzprofile aufgenommen worden, die regelmäßig veröffentlicht wird (siehe auch Internet: http://www.bsi.bund.de und [4]). Nähere Informationen sind über die BSI-Infoline +49 (0)228/9582-111 zu erhalten.

Unter der o. g. Internetadresse kann der Zertifizierungsreport in elektronischer Form abgerufen werden.

Der Auftraggeber[6] DB Netz AG hat einer Veröffentlichung der Zertifizierungsergebnisse zugestimmt.

[6] DB Netz AG
Mainzer Landstraße 201
60326 Frankfurt/M

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- dem zertifizierten Schutzprofil,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Schutzprofil Übersicht

Das Schutzprofil Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 [6] wurde entwickelt durch DB Netz AG als Vorlage für die Erstellung von Sicherheitsvorgaben, die im Rahmen der Zertifizierung eines IT-Produktes benötigt werden.

Das Schutzprofil definiert funktionale Anforderungen sowie Anforderungen an die Vertrauenswürdigkeit für die Module der Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA) der Deutschen Bahn.

Als Kernfunktion wird der TOE als Start- und Endpunkt einer kryptografisch gesicherten Verbindung (KISA-Verbindung) über offene Übertragungssysteme definiert. Die kryptografische Funktion und ihre unterstützenden Funktionseinheiten werden über gesicherte Managementverbindungen von mindestens einem zentralen Sicherheitscenter überwacht und betriebsgeführt.

Einsatzumgebung sind Bahnanwendungen und Systeme des Eisenbahnbetriebs. Es werden sicherheitsrelevante Nachrichten über offene Übertragungssysteme zwischen entfernten Orten des Eisenbahnbetriebs mit gleicher Integrität durch kryptografische Techniken gesichert.

Der TOE erbringt seine Sicherheitsdienste weitgehend automatisch. Informationsflüsse werden grundsätzlich durch die Bahnanwendung initiiert. Der TOE erlaubt ein **Management der Sicherheitsdienste** nach einer **Authentisierung** durch Benutzername und Passwort (oder einen gleich starken oder stärkeren Authentisierungsmechanismus) und die **Autorisierung** auf einzelne Objekte.

VPN-Client und Server (IPSec): Der TOE stellt einen **sicheren Kanal** mithilfe von IPSec (Internet Protocol Security) zwischen zwei oder mehreren Integritätsbereichen gleicher Sicherheit für die Kommunikation zwischen Bahnanwendungen bereit. Für jede Bahnanwendung wird ein sicherer Kanal initiiert. Der TOE prüft mittels Gültigkeit von Zertifikaten die **Authentizität** der Kommunikationspartner. Die Zertifikate werden mathematisch und gegen Sperrlisten geprüft. Für jede Sitzung wird ein Sitzungsschlüssel vereinbart. Der TOE löscht nicht mehr benötigte kryptographische Schlüssel nach ihrer Verwendung durch **aktives Überschreiben** aus seinem sicheren **Schlüsselspeicher**.

Der Nutzdatenstrom, welcher über den gesicherten Kanal übertragen wird, ist hinsichtlich seiner **Vertraulichkeit** und **Datenintegrität** geschützt. Zur Unterstützung des Ziels **Verfügbarkeit** wird innerhalb des TOEs der **Nutzdatenstrom priorisiert** weitergeleitet. Der TOE **protokolliert, mit Zeitstempel, und alarmiert** Ereignisse der Sicherheitsfunktionen. Zur Sicherstellung der Verfügbarkeit wird der TOE permanent überwacht und agiert operativ bei Beeinträchtigungen der Betriebsparameter. Der TOE setzt auch eine regelbasierte **Informationsflusskontrolle** um, d.h., regelbasiert müssen alle Informationsflüsse den etablierten sicheren Kanal nutzen.

Paketfilter: Der TOE bindet die Bahnanwendung sicher an offene Übertragungsnetze an. Dazu verfügt der TOE über die Funktionalität eines Paketfilters, welcher entsprechende Regeln umsetzen kann. Er schränkt die Menge der zulässigen Quellen und Ziele, Protokolle, Datendurchsatzraten ein. **Der TOE schützt sich selbst** und das lokale Netz der Bahnanwendung vor Angriffen aus dem offenen Übertragungsnetz und Angriffen aus dem lokalen Netz der Bahnanwendung. Der TOE beschränkt den freien Zugang zum

unsicher angesehenen offenen Übertragungsnetz zum Schutz des lokalen Netzes und der Bahnanwendung. Der TOE bietet **grundlegende Intrusion Detektion-Funktionalität**, womit nicht wohlgeformte IP-Pakete und einfache Angriffsmuster erkannt werden können.

Systemaktualisierungen: Für eine Reaktion auf erkannte Schwachstellen in der kryptografischen Funktion, weiteren Sicherheitsfunktionen oder der Systemsoftware kann aktualisierter Programmcode eingespielt werden.

Die Werte, die von einem zum Schutzprofil konformen Produkt (TOE) zu schützen sind, werden im Schutzprofil [6], Kapitel 3.1 aufgeführt. Basierend auf diesen Werten wird die Sicherheitsumgebung durch Annahmen, Bedrohungen und Organisatorische Sicherheitspolitiken definiert. Dies ist im Schutzprofil [6], Kapitel 3 dargestellt.

Diese Annahmen, Bedrohungen und Organisatorischen Sicherheitspolitiken werden auf Sicherheitsziele für einen TOE, der konform zum Schutzprofil ist, und auf Sicherheitsziele für die IT-Umgebung eines solchen TOEs abgebildet. Diese Ziele werden im Schutzprofil [6], Kapitel 4 beschrieben.

Das Schutzprofil verlangt, dass eine auf ihm basierende produktbezogene Sicherheitsvorgabe den Konformitätsgrad „strict“ erfüllt.

2 Funktionale Sicherheitsanforderungen

Ausgehend von den Sicherheitszielen, die ein EVG erfüllen muss für den die Komformität zu diesem Schutzprofil gefordert wird, ist die Sicherheitspolitik in Form von funktionalen Sicherheitsanforderungen (SFR), die ein EVG erfüllen muss, dargelegt.

Das Schutzprofil definiert funktionale Sicherheitsanforderungen in den Bereichen: FAU Security audit, FCS Cryptographic support, FDP User data protection, FIA Identification and authentication, FMT Security management und FPT Protection of the TSF.

Die funktionalen Sicherheitsanforderungen an einen TOE sind im Schutzprofil [6], Kapitel 5 enthalten. Sie sind alle den Common Criteria, Teil 2 entnommen. Das Schutzprofil ist daher bezüglich der funktionalen Sicherheitsanforderungen wie folgt gekennzeichnet:

PP conformant
Common Criteria Part 2 conformant

3 Anforderungen an die Vertrauenswürdigkeit

Das Paket von Vertrauenswürdigkeitskomponenten für ein Produkt, das dieses Schutzprofil erfüllen soll, ist komplett den Vertrauenswürdigkeitskomponenten aus Teil 3 der Common Criteria entnommen. Es lautet:

Common Criteria Teil 3 konform
EAL 4 mit Zusatz von
AVA_VAN.5

(zur Definition und zum Umfang der Vertrauenswürdigkeitspakete nach CC siehe [1] Teil 3).

4 Ergebnis der Schutzprofil-Evaluierung

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [5] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas

[3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Das Urteil PASS der Evaluierung wird für die Vertrauenswürdigkeitskomponenten der klasse APE bestätigt:

Im Einzelnen wurden die folgenden Vertrauenswürdigkeitskomponenten bewertet:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

Die Ergebnisse der Evaluierung gelten nur für das in Kapitel 1 definierte Schutzprofil.

5 Auflagen und Hinweise für den Gebrauch

Die folgenden Auflagen und Hinweise beim Gebrauch des Schutzprofil sind zu beachten:

- Im Schutzprofil sind zahlreiche Anwendungshinweise enthalten, die der Autor einer Produkt spezifischen Sicherheitsvorgabe beachten soll.

6 Schutzprofil Dokument

Das Schutzprofil Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 [6] wird als separates Dokument im Teil C: Anhang A zu diesem Zertifizierungsreport bereitgestellt.

7 Definitionen

7.1 Abkürzungen

AIS Anwendungshinweise und Interpretationen zum Schema

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

ETR Evaluation Technical Report

EVG Evaluierungsgegenstand (target of evaluation)

IT Informationstechnik

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility - Prüfstelle

PP Protection Profile - Schutzprofil

SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy - EVG Sicherheitspolitik
SFR	Security Functional Requirement - funktionale Sichertheitsanforderungen
ST	Security Target - Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSF	TOE Security Functionality - EVG Sicherheitsfunktionalität

7.2 Glossar

Erweiterung (extension) - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind.

Evaluationsgegenstand (target of evaluation) - Software, Firmware und / oder Hardware und zugehörige Handbücher.

EVG-Sicherheitsfunktionalität (TOE security functionality) - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die SFR durchzusetzen.

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

Informell (informal) - Ausgedrückt in natürlicher Sprache.

Objekt (object) - Eine passive Einheit im EVG, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil (protection profile) - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

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

Sicherheitsvorgaben (security target) - Eine implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Subjekt (subject) - Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

Zusatz (augmentation) - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

8 Literaturangaben

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012 http://www.commoncriteriaportal.org

[3] BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für das Schutzprofil relevant sind[7]

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird

[5] Evaluation Technical Report, Version 1.8, Date 08.07.2016, Evaluation Report, SRC Security Research & Consulting GmbH (confidential document)

[6] Common Criteria Schutzprofil (Protection Profile) für KISA-Module, Anforderungen an die Kommunikationsinfrastruktur für sicherheitsrelevante Anwendungen (KISA), PP0085, Version 1.0, Datum 25. Juli 2016, DB Netz AG

[7] insbesondere

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)

C Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Schutzprofil Anforderungen an die Kommunikationsinfrastrukur für sicherheitsrelevante Anwendungen (KISA), Version 1.0 [6] wird in einem eigenen Dokument zur Verfügung gestellt.

Bemerkung: Ende des Reportes