Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-CC-PP-0033-2007

zu

Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor Version 1.05

entwickelt durch das

Bundesamt für Sicherheit in der Informationstechnik

im Auftrag des

Bundesministerium für Gesundheit

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0033-2007

Common Criteria Schutzprofil

Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor
Version 1.05

Common Criteria Arrangement

entwickelt durch Bundesamt für Sicherheit in der Informationstechnik
im Auftrag von Bundesministerium für Gesundheit

Vertrauenswürdigkeitspaket des Schutzprofiles:
Common Criteria Teil 3 konform
EAL 4 mit Zusatz von
ADV_IMP.2 – Implementierung der TSF
AVA_MSU.3 – Analysieren und Testen auf unsichere Zustände
AVA_VLA.4 – Hohe Widerstandsfähigkeit

Common Criteria

Das Schutzprofil wurde von einer akkreditierten und lizenzierten Prüfstelle unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3* in Übereinstimmung mit den *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)* 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 einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, verbunden.

Bonn, 9. Oktober 2007

Der Vizepräsident des Bundesamtes
für Sicherheit in der Informationstechnik

Hange

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

Dies ist eine eingefügte Leerseite.

Vorbemerkungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] neben der Zertifizierung von Sicherheitsprodukten für die 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 geschieht auf Veranlassung des BSI oder eines Antragstellers. Antragsteller können IT-Hersteller oder IT-Anwender sein.

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 selbst durchgeführt.

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

---

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)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3[6]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Verfahren der Erteilung eines PP-Zertifikats durch das BSI.

2 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von Zertifikaten für Schutzprofile auf Basis der Common Criteria unter gewissen Bedingungen vereinbart.

---

[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 3. März 2005, Bundesgesetzblatt I S. 519

[6] Bekanntmachung des Bundesministeriums des Innern vom 10. Mai 2006 im Bundesanzeiger, datiert 19. Mai 2006, S. 19445

2.1 Internationale Anerkennung von CC - Zertifikaten

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 verabschiedet (CC-MRA). Diese Vereinbarung schließt die Anerkennung von Schutzprofilen auf Basis der CC ein.

Der Vereinbarung sind bis Februar 2007 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn, USA. Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.commoncriteriaportal.org eingesehen werden.

Das Logo der Common-Criteria-Vereinbarung auf dem Zertifikat zeigt, dass dieses Zertifikat unter die Anerkennungsvereinbarung fällt.

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 Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 hat das Zertifizierungsverfahren beim BSI durchlaufen. Die Evaluierung wurde am 07. September 2007 beendet.

Die Evaluierung des Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 wurde von der media transfer AG durchgeführt. Das Prüflabor media transfer AG ist eine vom BSI anerkannte Prüfstelle (ITSEF)[7].

Der Antragsteller für diese Zertifizierung ist:

Bundesministerium für Gesundheit

Den Abschluss der Zertifizierung bilden die Vergleichbarkeitsprüfung und die Erstellung des vorliegenden Zertifizierungsreports durch das BSI.

4 Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die oben angegebene Version des Protection Profiles.

---

[7] Information Technology Security Evaluation Facility

Die Gültigkeit kann auf neue Versionen des Protection Profiles 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 Vertrauenswürdigkeitsstufen und die Stärke der Funktionen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports erläutert.

5 Veröffentlichung

Der folgende Zertifizierungsbericht umfasst die Seiten B-1 bis B-7.

Das Schutzprofil Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 ist in die BSI-Liste der zertifizierten Schutzprofile aufgenommen worden, die regelmäßig veröffentlicht wird (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline +49 (0)228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Entwickler[8] des Protection Profile angefordert werden. Unter der o. g. Internet-adresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[8] Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

Dies ist eine eingefügte Leerseite.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- dem zur Zertifizierung vorgelegten Protection Profile,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

Gliederung des Zertifizierungsberichts

1 Protection Profile Übersicht

Das Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 wurde im Auftrag des Bundesministerium für Gesundheit erstellt und dient als Grundlage für die Entwicklung von Security Targets zur Zertifizierung von IT-Produkten. Es beschreibt die Sicherheitsanforderungen für einen Netzkonnektor im elektronischen Gesundheitswesen. Ein Netzkonnektor ist dabei Teil eines Konnektors im elektronischen Gesundheitswesen, zu dem zusätzlich zum Netzkonnektor noch ein Anwendungskonnektor gehört.

Ein Konnektor bildet die Schnittstelle zwischen den dezentralen Primärsystemen und der zentralen Telematikinfrastruktur des Gesundheitswesens. Zu den dezentralen Primärsystemen des Gesundheitswesens zählen u. a. die Verwaltungssysteme in Arztpraxen, Apotheken und Krankenhäuser. Zur zentralen Telematikinfrastruktur des Gesundheitswesens zählen alle Instanzen, welche die Fachdienste des Gesundheitswesens erbringen und bereitstellen. Die im Gesundheitswesen für einen Konnektor insgesamt maßgeblichen Funktionen und Schnittstellen sind in der Konnektor-Spezifikation [8] beschrieben.

Das Schutzprofil extrahiert die sich aus der Konnektor-Spezifikation [8] ergebenden Sicherheitsanforderungen an den Netzkonnektor. Der Netzkonnektor verbindet die dezentralen Primärsysteme sicher mit der zentralen Telematikinfrastruktur. Er realisiert die sichere Verbindung zwischen den Instanzen durch den Aufbau einer VPN-Verbindung zu einem VPN-Konzentrator auf der Basis des IPSec-Protokolls über ein Transportnetz (z.B. das Internet). Die kommunizierenden Instanzen authentifizieren sich gegenseitig und übertragen die zu schützenden Daten signiert und verschlüsselt. Der Netzkonnektor stellt im Wesentlichen eine dynamische Paketfilterfunktionalität und die Leistungen eines VPN-Clients zur Verfügung.

Die Sicherheitsanforderungen für den Anwendungskonnektor werden in einem separaten Schutzprofil beschrieben.

Die Werte, die von einem zum PP konformen Produkt (TOE) zu schützen sind, werden im Protection Profile [7], Kapitel 3 aufgeführt. Basierend auf diesen Werten wird die Sicherheitsumgebung durch Annahmen und Bedrohungen im selben Kapitel spezifiziert.

Diese Annahmen und Bedrohungen werden auf Sicherheitsziele für einen TOE, der konform zum PP ist, und auf Sicherheitsziele für die IT-Umgebung eines solchen TOE abgebildet. Diese Ziele werden im PP [7], Kapitel 4 beschrieben.

2 Funktionale Sicherheitsanforderungen

Die Sicherheitsziele für einen TOE, der konform zum PP ist, werden durch eine Menge von funktionalen Sicherheitsanforderungen (SFR) erfüllt. Diese müssen

von einem zum PP konformen TOE umgesetzt werden und somit den folgenden Sicherheitspolitiken gerecht werden:

- Sicherstellung der Integrität und der Vertraulichkeit bei der Übermittlung von medizinischen oder sonstigen personenbezogenen Daten über das Transportnetz,
- Schutz der Primärsysteme vor Angriffen aus dem Transportnetz und
- Bereitstellung von sicheren Möglichkeiten zur Administration und zur Aktualisierung der Firmware.

Die funktionalen Sicherheitsanforderungen an einen TOE sind im PP [7], Kapitel 5 enthalten. Sie wurden den Common Criteria, Teil 2 entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Das Protection Profile ist daher bezüglich der funktionalen Sicherheitsanforderungen wie folgt gekennzeichnet:

Common Criteria Teil 2 erweitert

3 Anforderungen an die Vertrauenswürdigkeit

Das Paket von Vertrauenswürdigkeitskomponenten für dieses Protection Profile ist komplett den Vertrauenswürdigkeitskomponenten aus Teil 3 der Common Criteria entnommen. Das Vertrauenswürdigkeitspaket lautet daher:

Common Criteria Teil 3 konform
EAL 4 mit Zusatz von
ADV_IMP.2 – Implementierung der TSF
AVA_MSU.3 – Analysieren und Testen auf unsichere Zustände
AVA_VLA.4 – Hohe Widerstandsfähigkeit

(Zur Definition und dem Umfang von Vertrauenswürdigkeitspaketen gemäß den Common Criteria siehe Teil C or [1], Teil 3).

4 Ergebnis der PP-Evaluation

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [6] 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.

Das Ergebnis der Evaluierung lautet “PASS” für die Vertrauenswürdigkeits-komponenten der Klasse APE.

Im Einzelnen wurden die folgenden Vertrauenswürdigkeitskomponenten bewertet:

APE_INT.1 - PP introduction (PP-Einführung)
APE_DES.1 - TOE description (EVG-Beschreibung)
APE_ENV.1 - Security environment (Sicherheitsumgebung)
APE_OBJ.1 - Security objectives (Sicherheitsziele)

APE_SRE.1 - Explicitly stated IT security requirements
(Explizit dargelegte IT-Sicherheitsanforderungen)
APE_REQ.1 - IT security requirements (IT-Sicherheitsanforderungen)

Die Ergebnisse der Evaluierung sind nur anwendbar für die Version des Protection Profile, die im Kapitel 1 angegeben ist.

5 Auflagen und Hinweise für den Gebrauch

Die folgenden Hinweise beim Gebrauch des Protection Profile sind zu beachten:

Die verbindlichen Inhalte im Schutzprofil sind auf die Minimalanforderungen an den Netzkonnektor beschränkt. Jede spezielle Ausprägung des Netzkonnektors kann zusätzliche Sicherheitsanforderungen nach sich ziehen. Weiterhin ist es möglich, dass Produkte über zusätzliche Sicherheitsleistungen Alleinstellungsmerkmale bereitstellen. Wo dies bereits absehbar ist, wird der Anwender bzw. Leser in diesem Schutzprofil in Form von Application Notes darauf hingewiesen, in einem Security Target entsprechende Ergänzungen vorzunehmen.

6 Protection Profile Dokument

Das Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 [7] wird als separates Dokument im Teil D: Anhänge, Anhang A zu diesem Zertifizierungsbericht bereitgestellt.

7 Definitionen

7.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn

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

CCRA Common Criteria Recognition Arrangement

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluationsgegenstand - TOE: Target of Evaluation

IT Informationstechnik

ITSEF Information Technology Security Evaluation Facility - Prüfstelle

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SFP Security Function Policy - Funktionale Sicherheitspolitk

SOF Strength of Function - Stärke der Funktionen

ST	Security Target - Sicherheitsvorgaben
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions - EVG-Sicherheitsfunktionen
TSP	TOE security policy - EVG-Sicherheitspolitik

7.2 Glossar

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

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind, zu den Sicherheitsvorgaben bzw. dem Schutzprofil.

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.

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 Anwenderbedürfnisse erfüllen.

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

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.

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.

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-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.

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.

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

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

8 Literaturangaben

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

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

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird

[6] Evaluierungsendbericht, Version 1.04, 14.08.2007, „Evaluation Technical Report Zusammenfassung“, media transfer AG (vertrauliches Dokument)

[7] Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05, 04.09.2007, Bundesamt für Sicherheit in der Informationstechnik

[8] Einführung der Gesundheitskarte: Konnektorspezifikation, Version 2.0.0, 04.05.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

C Auszüge aus den technischen Regelwerken

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 2.3 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Anhänge

Liste der Anhänge in diesem Zertifizierungsreport

Anhang A: Protection Profile Konnektor im elektronischen Gesundheitswesen, Anforderungen an den Netzkonnektor, Version 1.05 [7] bereitgestellt in einem separaten Dokument.

Dies ist eine eingefügte Leerseite.