Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0282-2006

zu

Gefäßidentifikationssystem BiTech bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern

der

deister electronic GmbH

BSI- Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49(0)3018 9582-0, Telefax +49(0)3018 9582-5455, Infoline +49(0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0282-2006

Gefäßidentifikationssystem BiTech bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern

Common Criteria Arrangement

der

deister electronic GmbH

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3 (ISO/IEC 15408:2005),* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 (ISO/IEC 15408:2005)* evaluiert.

Prüfergebnis:

PP-Konformität:	**Schutzprofil BSI-PP-0010-2004**
Funktionalität:	**BSI-PP-0010-2004 konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert**
Vertrauenswürdigkeit:	**Common Criteria Teil 3 konform EAL 1**

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration 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 sind in Einklang mit den erbrachten Nachweisen.

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 24. August 2006

Der Vizepräsident des Bundesamtes für Sicherheit
in der Informationstechnik

Hange L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt 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.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

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

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom 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 Produktes, 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

Gliederung

Teil A: Zertifizierung

Teil B: Zertifizierungsbericht

Teil C: Auszüge aus den technischen Regelwerken

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG[2]
- BSI-Zertifizierungsverordnung[3]
- BSI-Kostenverordnung[4]
- 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[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)

---

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

[3] 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

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

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

2 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart. Zertifikate der Unterzeichnerstaaten werden damit in den jeweils anderen Unterzeichnerstaaten anerkannt.

2.1 ITSEC/CC - Zertifikate

Das SOGIS-Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf Grundlage der ITSEC, ist am 03. März 1998 in Kraft getreten. Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert.

2.2 CC - Zertifikate

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-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. Im November 2000 ist Israel der Vereinbarung beigetreten, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003, Japan im November 2003, die Tschechische Republik im September 2004, die Republik Singapore im März 2005, Indien im April 2005.

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 Produkt Gefäßidentifikationssystem BiTech, bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Gefäßidentifikationssystem BiTech wurde von der CSC Deutschland Solutions GmbH durchgeführt. Das Prüflabor CSC Deutschland Solutions GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller, Hersteller und Vertreiber ist

deister electronic GmbH
Hermann-Bahlsen-Straße 11 – 13
30890 Barsinghausen.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 24. August 2006 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, daß

- alle Auflagen bzgl. Generierung, Konfiguration und Betrieb, soweit sie im nachfolgenden Bericht angegeben sind, beachtet werden,
- das Produkt in der beschriebenen Umgebung - sofern im nachfolgenden Bericht angegeben - betrieben wird.

Dieser Zertifizierungssreport gilt nur für die hier angegebene Version des Produktes. Die Gültigkeit kann auf neue Versionen und Releases des Produktes ausgedehnt werden, sofern der Antragsteller eine Re-Zertifizierung des geänderten Produktes entsprechend den Vorgaben beantragt und die Prüfung keine sicherheitstechnischen Mängel ergibt.

Hinsichtlich der Bedeutung der Vertrauenswürdigkeitsstufen und der bestätigten Stärke der Funktionen vgl. die Auszüge aus den technischen Regelwerken am Ende des Zertifizierungsreports.

[6] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-18.

Das Produkt Gefäßidentifikationssystem BiTech ist in die BSI-Liste der zertifizierten Produkte, 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 Hersteller[7] des Produktes angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsroeprt auch in elektronischer Form abgerufen werden.

[7] deister electronic GmbH
Hermann-Bahlsen-Straße 11 – 13
30890 Barsinghausen

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

Gliederung des Zertifizierungsberichtes

1	Zusammenfassung	3
2	Identifikation des EVG	8
3	Sicherheitspolitik	10
4	Annahmen und Klärung des Einsatzbereiches	10
5	Informationen zur Architektur	12
6	Dokumentation	12
7	Testverfahren	13
8	Evaluierte Konfiguration	14
9	Ergebnisse der Evaluierung	14
10	Kommentare und Empfehlungen	15
11	Anhänge	15
12	Sicherheitsvorgaben	15
13	Definitionen	16
14	Literaturangaben	18

1 Zusammenfassung

Beim EVG handelt es sich um das Gefäßidentifikationssystem BiTech, bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern (ID-Tags) der Firma deister electronic GmbH. Dieser EVG ist konform zum Schutzprofil „Protection Profile Waste Bin Identification System (WBIS-PP), Version 1.04“ [8] evaluiert worden.

Abfallbehälter-Identifikations-Systeme (WBIS) im Sinne dieses Dokumentes sind Systeme, durch die Abfallbehälter mit einem ID-Tag (z.B. mit elektronischem Chip, dem Transponder) identifiziert werden, um feststellen zu können, wie oft der einzelne Abfallbehälter geleert worden ist. Dabei handelt es sich bei diesen Systemen nicht um die direkte Identifizierung von Abfällen, sondern um die Identifizierung der Behälter, in denen Abfälle zur Entsorgung bereitgestellt werden.

Der EVG prüft dazu die vom Transponder eingelesen Daten auf Integrität, ergänzt korrekte Daten durch Datum und Uhrzeit der Leerung, fügt ein Gültigkeits- sowie ein Intergritätsmerkmal an und speichert diese Daten dann redundant auf zwei getrennten Speichern im Fahrzeugrechner, damit diese auch bei einem Verlust der Daten im ersten Speicher wiederhergestellt werden können. Bei der Übertragung in die Bürosoftware prüft der EVG im Sicherheitsmodul die Daten erneut auf Gültigkeit und Integrität und kennzeichnet diese entsprechend.

Damit ist der EVG in der Lage, die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vom Transponder bis in die Bürosoftware vor Manipulation und Verlust zu schützen.

Die Evaluation des Produktes Gefäßidentifikationssystem BiTech, bestehend aus den Transpondern (ID-Tags) (Artikelnummern siehe Kapitel 2, Tabelle 2 dieses Reports), sowie der zertifizierten Komponente „DE_BSI_M16_LIB, Version 1.5“ der Fahrzeugsoftware und dem Sicherheitsmodul „DE_BSI_PC_DLL, Version 1.5“ als Teil der Bürosoftware, wurde von CSC Deutschland Solutions GmbH durchgeführt und am 19. Juli 2006 abgeschlossen. Das Prüflabor CSC Deutschland Solutions GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[8].

Antragsteller, Hersteller und Vertreiber ist

deister electronic GmbH
Hermann-Bahlsen-Straße 11 – 13
30890 Barsinghausen.

[8] Information Technology Security Evaluation Facility

1.1 Vertrauenswürdigkeitspaket

Die Vertrauenswürdigkeitskomponenten des EVG sind konform zum Teil 3 der CC [1]. Der EVG wurde erfolgreich mit der Prüfstufe EAL1 (funktionell getestet) evaluiert (siehe auch Annex C oder [1], Teil 3). In Kapitel 9, Tabelle 6 dieses Reports sind die gewählten Vertrauenswürdigkeitskomponenten mit dem Evaluierungsergebnis detailliert aufgeführt.

1.2 Funktionalität

Die im Schutzprofil ausgewählten und in die Sicherheitsvorgaben übernommenen funktionalen Sicherheitsanforderungen (SFR – Security Functional Requirements) sind CC,Teil 2 erweitert. Die Auflistung in der folgenden Tabelle zeigt die zu Teil 2 der CC konformen SFRs:

Funktionale Sicherheitsanforderungen	**Bedeutung**
FDP	**Schutz der Benutzerdaten**
FDP_DAU.1	Einfache Datenauthentisierung
FDP_SDI.1	Überwachung der Integrität der gespeicherten Daten
FRU	**Betriebsmittelnutzung**
FRU_FLT.1	Verminderte Fehlertoleranz

Tabelle 1: SFRs des EVG CC, Teil 2 konform

Die Auflistung in Tabelle 2 zeigt die explizit dargelegten (Teil 3 erweiterten) SFRs:

Funktionale Sicherheitsanforderungen	**Bedeutung**
FDP	**Schutz der Benutzerdaten**
FDP_ITT.5	Interne Transferintegrität

Tabelle 2: SFRs des EVG CC, Teil 2 erweitert

Hinweis: Es werden nur die Titel der SFRs genannt. Detailiertere Informationen befinden sich in Kapitel 6.1 der Sicherheitsvorgaben [6].

Die funktionalen Sicherheitsanforderungen werden durch folgende Sicherheitsfunktionen umgesetzt:

TSF_IDCHK Funktion, die aufgrund von übergebenen Identifikationsdaten AT1 aus dem Transponder (ID-Tag) mit anhängendem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) an den "nicht EVG-pflichtigen Teil der Fahrzeugsoftware" übergibt. Bei diesem Ergebnis handelt es sich um eine Information, ob der aus dem Transponder eingelesene CRC-Wert mit dem aktuellen durch den EVG berechneten CRC-Wert übereinstimmt.

TSF_BSU-KEN Funktion, die in einen neu angelegten Leerungsdatenblock AT+ die Kennung des angeschlossenen Fahrzeugrechners (BSU) schreibt. In jeden neu angelegten Leerungsdatenblock AT+ wird die Kennung der BSU ausgelesen und sofort eingefügt. Bei einem Wechsel der Kennung wird ein ggf. offener Leerungsdatenblock sofort abgeschlossen und ein neuer AT+ mit der nun aktuellen Kennung angelegt.

TSF_AT+CRC Funktion, die über einen gültigen Leerungsdatenblock AT+, bestehend aus Leerungsdatensätzen AT den CRC-Wert berechnet und diesen CRC-Wert dem Leerungsdatenblock anhängt.

TSF_SAFE Funktion, die die Leerungsdatenblöcke AT+ im primären und sekundären Speicher ablegt und wieder ausliest.

TSF_BSU-CHK Funktion, die die Gültigkeit der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatenblöcke AT+ überprüft.

TSF_AT+CHK Funktion, die aufgrund der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatenblöcken AT+ mit beigefügtem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) anzeigt. Bei diesem Ergebnis handelt es sich um eine Information, ob der auf dem Fahrzeugrechner für den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze AT erzeugte CRC-Wert mit dem aktuellen, durch den EVG berechneten CRC-Wert übereinstimmt. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheitsmodul für die korrekte Weiterverarbeitung genutzt.

1.3 Stärke der Funktionen

Da der EVG vor allem gegen unabsichtliche oder zufällige Veränderungen und Verluste von Daten, z.B. durch technische Effekte, wie Handystrahlung, wirkt, genügt für seine Prüfung zunächst die Vertrauenswürdigkeitsstufe EAL1. Diese enthält keine Familien der Klasse AVA, insbesondere keine Komponenten der Familie AVA_SOF „Stärke der Sicherheitsfunktionen“. Postulate zur EVG-Funktionsstärke sind somit nicht erforderlich.

1.4 Zusammenfassung der Bedrohungen und der organisatorischen Sicherheitspolitik, auf die das evaluierte Produkt ausgerichtet ist

Nachfolgend werden zunächst die schutzwürdigen Objekte, die Subjekte und die Urheber von Bedrohungen definiert.

Schutzwürdige Objekte sind

- Leerungsdatensätze AT zu einer Leerung
  Ein Leerungsdatensatz AT besteht aus den Datenfeldern AT1, Identifikationsdaten des Abfallbehälters und AT2, Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.
- Leerungsdatenblöcke AT+
  In einem Leerungsdatenblock werden bis zu zehn Leerungsdatensätze zusammengefasst.

Subjekte des EVG im Sinne der CC sind vertrauenswürdige Personen (S.Trusted) im Umfeld des EVG. Dies sind die Besatzungen der Fahrzeuge, die Benutzer der Bürorechner und Personen, die das System installieren oder warten, sowie die Personen, die für die Sicherheit der Umgebung verantwortlich sind.
Urheber von Bedrohungen sind Angreifer (S.Attack), deren Hauptziel es ist, sensitive Daten der Anwendung zu modifizieren oder zu verfälschen. Angreifer des EVG verfügen höchstens über Kenntnisse offensichtlicher Schwachstellen.

Aufgrund der obigen Definitionen wurden folgende Bedrohungen identifiziert, denen der EVG entgegenwirken muss:

- T.Man Manipulierte Identifikationsdaten
  Ein Angreifer (S.Attack) manipuliert die Identifizierungsdaten AT1 im ID-Tag durch Mittel (z.B. mechanische Einwirkung), die die Identifizierungsdaten AT1 ausschließlich rein zufällig verfälschen.
- T.Jam#1 Gestörte Identifikationsdaten
  Ein Angreifer (S.Attack) stört die Übertragung der Identifizierungsdaten AT1 vom ID-Tag zum Leser im Fahrzeug durch Mittel (z.B. elektromagnetische Strahlung), die die Identifizierungsdaten AT1 ausschließlich rein zufällig verfälschen.
- T.Create Ungültige Leerungsdatenblöcke
  Ein Angreifer (S.Attack) erzeugt beliebige Leerungsdatenblöcke AT+ und überträgt diese an das Sicherheitsmodul.
- T.Jam#2 Verfälschte Leerungsdatensätze
  Ein Angreifer (S.Attack) verfälscht Leerungsdatensätze AT während der Bearbeitung und der Speicherung innerhalb des Fahrzeuges oder stört die Übertragung der Leerungsdatenblöcke AT+ von der Fahrzeugsoftware zum Sicherheitsmodul z.B. durch elektromagnetische Strahlung, um die Daten der Leerungsdatenblöcke AT+ ausschließlich rein zufällig zu verfälschen.

In Ergänzung zur Abwehr der Bedrohungen soll der EVG die folgende Sicherheitspolitik unterstützen:

- P.Safe Fehlertoleranz
  Die Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblöcke AT+ durch eine redundante Speicherung in einem sekundären Speicher so geschützt sind, dass die Übertragung der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul nach einem Verlust der Daten in einem primären Speicher möglich ist.

1.5 Spezielle Konfigurationsanforderungen

Der EVG-Teil der Fahrzeugsoftware wird zusammen mit der Firmware des Fahrzeugrechners vom Hersteller nach Kundenwunsch vorkonfiguriert. Die Konfiguration der Bürosoftware und des Sicherheitsmoduls wird im „BiDIP2 Installations- und Benutzerhandbuch“ [10] detailliert beschrieben.

1.6 Annahmen über die Einsatzumgebung

Für den EVG werden folgende Annahmen an die Einsatzumgebung gestellt:

Annahme	Inhalt
A.Id	ID-Tag
A.Trusted	Vertrauenswürdiges Personal
A.Access	Zugangsschutz
A.Check	Überprüfung der Vollständigkeit
A.Backup	Datensicherung
A.Installation	Korrekte Inbetriebnahme

Tabelle 3: Annahmen an die Einsatzumgebung

Hinweis: An dieser Stelle werden nur die Titel der Annahmen genannt. Detailliertere Informationen befinden sich in Kapitel 4 dieses Reports und in Kapitel 4.1 der Sicherheitsvorgaben [6]. Die Annahme A.Installation wurde in den Sicherheitsvorgaben gegenüber dem Schutzprofil ergänzt.

1.7 Gewährleistungsausschluß

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt 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.

2 Identifikation des EVG

Der EVG heisst:

Gefäßidentifikationssystem BiTech, bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern

Er besteht aus folgenden Komponenten:

Nr.	Typ	Bezeichnung	Version	Anmerkungen
1	HW / SW	Transponder (ID-Tags)	Artikelnummern: 8101.710, 8101.711, 8101.910, 8101.911, 8101.501, 8111.501, 8102.700, 8102.701, 8102.501, 8103.501, 8103.910, 8103.911, 8104.700, 8104.701, 8104.501, 8105.700, 8105.701, 8105.501, 8107.700, 8107.701	Bei den ID-Tags handelt es sich um passive Transponder, die am oder im zu identifizierenden Gegenstand befestigt werden. Alle Transponder besitzen eine unique ID mit einer Datenstruktur von mind. 64 Bit und sind sowohl nur lesbar (Read Only und OTP) als auch les- und beschreibbar (Read/Write), wobei die unique ID unveränderbar ist. Der beschreibbare Teil des Transponders ist nicht Teil des EVG.
2	SW	EVG-Teil der Fahrzeugsoftware	DE_BSI_M16_LIB, Version 1.5 Dateien: DE_BSI_M16_LIB.A und DE_BSI_M16_LIB.H	Anmerkung: Diese Library wird zusammen mit der BSU Firmware DE_BSU auf einem von der Firma deister electronic entwickelten Fahrzeugrechner (BSU) betrieben, basierend auf einem Mikroprozessor der MC16 Familie von Mitsubishi.
3	DOK	Gefäßidentifikations-system Installations- und Benutzerhandbuch	Version 27/06/06	
4	SW	Sicherheitsmodul	DE_BSI_PC_DLL, Version 1.5 Dateien: DE_BSI_PC_DLL.DLL und DE_BSI_PC_DLL.H	Bei dem Sicherheitsmodul handelt sich um den EVG-Teil der Bürosoftware. Dieses Modul muss in die Bürosoftware eingebunden werden, die nicht Bestandteil des EVG ist.
5	DOK	BiDIP2 Installations- und Benutzerhandbuch	Version 27/06/06	

Tabelle 4: Komponenten des EVG

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr.	Typ	Bezeichnung	Version	Form der Auslieferung
1	HW	Transponder (ID-Tags)	(siehe Tabelle **4**)	
2	SW	Firmware in der BSU: BSU mit Firmware BSU_CAN_8V2_57.HE_ (nicht Bestandteil des EVG) Beinhaltet: DE_BSI_M16_LIB.A	 Version 2.57 Version 1.5	Installiert auf dem Fahrzeugrechner
3	DOK	Gefäßidentifikations-system Installations- und Benutzerhandbuch [9]	Version 27/06/06	CD
4	SW	Bürosoftware mit Sicherheitsmodul: Bürosoftware BiDIP Sicherheitsmodul DE_BSI_PC_DLL.	 Version 2.0.1 Version 1.5	CD
5	DOK	BiDIP2 Installations- und Benutzerhandbuch [10]	Version 27/06/06	CD
6	DOK	Handheld BHT, BHT lite, BHI, BHI Pro Manual [11]	Version 20/09/05	CD

Tabelle 5: Auslieferungsumfang des EVG

Der EVG-Teil der Fahrzeugsoftware wird vom Hersteller als Teil der Firmware in der BSU auf dem Fahrzeug installiert und zusammen mit dieser ausgeliefert. Die Versionsabfrage zum EVG-Teil der Fahrzeugsoftware ist im Handbuch zur Fahrzeugsoftware [9] beschrieben.

Das Sicherheitsmodul wird zusammen mit der Bürosoftware auf einer CD ausgeliefert und an den Kunden versendet.
Der Anwender kann sich den Namen und die Version des installierten Sicherheitsmoduls anzeigen lassen um sicherzustellen, dass das zertifizierte Modul verwendet wird. Die Versionsabfrage ist im Handbuch zur Bürosoftware [10] beschrieben.

Die Handbücher werden ebenfalls auf der gleichen CD ausgeliefert.

3 Sicherheitspolitik

Der EVG soll Manipulationen an den, in einem ID-Tag gespeicherten Identifikationsdaten während der Speicherung im ID-Tag und der Übertragung zwischen ID-Tag und Leser erkennen.

Er soll Manipulationen an empfangenen Leerungsdatensätzen während des Leerungsprozesses und Speicherns im Fahrzeug erkennen, sowie Manipulationen der Leerungsdatenblöcke bei zufälligen Störungen während des Transfers von der Fahrzeugsoftware zum Sicherheitsmodul.

Der EVG soll sicherstellen, dass die Daten redundant in einem sekundären Speicher gesichert werden. So ist der Transfer der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul auch noch möglich, sofern Leerungsdatenblöcke im Primärspeicher der Fahrzeugsoftware verloren gehen.

Er soll jeden Versuch einer Übermittlung willkürlicher (z.B. ungültiger) Leerungsdatenblöcke an das Sicherheitsmodul erkennen.

4 Annahmen und Klärung des Einsatzbereiches

4.1 Annahmen über den Einsatz

A.Trusted:
Die Besatzung des Fahrzeugs und die Benutzer des Bürorechners (S.Trusted) sind autorisiert und vertauenswürdig. Alle Personen, die das System installieren, initialisieren oder warten sind autorisiert und vertrauenswürdig (S.Trusted). Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind (S.Trusted), sind autorisiert und vertrauenswürdig.

A.Check:
Der Benutzer prüft in regelmäßigen Abständen, ob alle Leerungsdatenblöcke AT+ von dem Fahrzeugrechner übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer (S.Trusted) in einem bestimmten Zeitraum durch erneutes Abrufen beim Fahrzeugrechner behoben. Dieser Zeitraum entspricht der Kapazität des jeweiligen Speichers im Fahrzeugrechner, der zur Speicherung der Leerungsdatenblöcke AT+ zur Verfügung steht.

A.Backup:
Der Benutzer (S.Trusted) sichert die vom Evaluierungsgegenstand erzeugten Daten regelmäßig im Archiv. Der Evaluierungsgegenstand schützt nicht vor Datenverlusten im Archiv.

A.Installation:
Bei Installation des Identifikationssystemes auf dem Fahrzeug wird sichergestellt, dass die BSU-Kennung und die Adressen der Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

4.2 Angenommene Einsatzumgebung

A.Id:
Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten AT1 des Abfallbehälters sind in dem ID-Tag gespeichert und werksseitig durch einen CRC geschützt. Es werden nur ID-Tags mit einmaligen Identifizierungsdaten installiert. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.

A.Access:
Die Umgebung stellt durch geeignete Maßnahmen (Verschluss, Zugangskontrolle durch Passwörter usw.) sicher, dass nur der Benutzer bzw. das Wartungspersonal (S.Trusted) direkten Zugang zu allen Komponenten des Evaluierungsgegenstands, ausgenommen der ID-Tag, haben. Die Beeinflussung der internen Verbindungskanäle innerhalb der IT-Struktur des Bürorechners durch einen potenziellen Angreifer (S.Attack) ist aufgrund geeigneter Maßnahmen ausgeschlossen.

4.3 Klärung des Einsatzbereiches

Der EVG gewährleistet mit seinen Sicherheitsfunktionen die Integrität und Vollständigkeit der zu schützenden Daten. Er gewährleistet jedoch nicht die Vertraulichkeit der Daten, dass heisst er beinhaltet keine Funktionalität zur Verschlüsselung.

Der EVG beinhaltet die Softwarekomponente DE_BSI_M16_LIB Version 1.5 als Teil der Fahrzeugsoftware. Der EVG-Teil der Fahrzeugsoftware prüft die vom Transponder eingelesen Daten auf Integrität, ergänzt korrekte Daten durch Datum und Uhrzeit der Leerung, fügt ein Gültigkeits- sowie ein Integritätsmerkmal an und speichert diese Daten dann redundant auf zwei getrennten Speichern im Fahrzeugrechner. Jegliche weitere Funktionalität der Fahrzeugsoftware ist nicht Bestandteil der Zertifizierung. Die Speicher gehören ebenfalls nicht zum EVG. Sie bestehen aus dem SRAM-Speicher der BSU als Primärspeicher und einer Speicher-Flashkarte (PCMCIA-Karte) als Sekundärspeicher.

Die Daten werden über einen mobilen Datenträger (z.B. Handheld, Speicherbox, CE-terminal) von der BSU in das Sicherheitsmodul übertragen. Die mobilen Datenträger sind nicht Bestandteil der Zertifizierung.

Des Weiteren beinhaltet der EVG das Sicherheitsmodul, die Software-Komponente DE_BSI_PC_DLL Version 1.5 als Teil der Bürosoftware. Das Sicherheitsmodul prüft die Daten erneut auf Gültigkeit und Integrität und kennzeichnet diese entsprechend für die Weiterverarbeitung. Jegliche weitere Funktionalität der Bürosoftware ist nicht Bestandteil der Zertifizierung.

Ebenfalls zum EVG gehören die Transponder (ID-Tags) mit den durch CRC-Checksummen gegen Manipulationen geschützen Identifikationsdaten.

5 Informationen zur Architektur

Da dieser EVG lediglich auf der Stufe EAL 1 evaluiert wurde, gibt es keine Architekturbeschreibung (High Level Design), die die Komponenten des EVG beschreibt.

Die folgende Abbildung gibt jedoch einen Überblick über das Abfallbehälter-Identifikations-System.

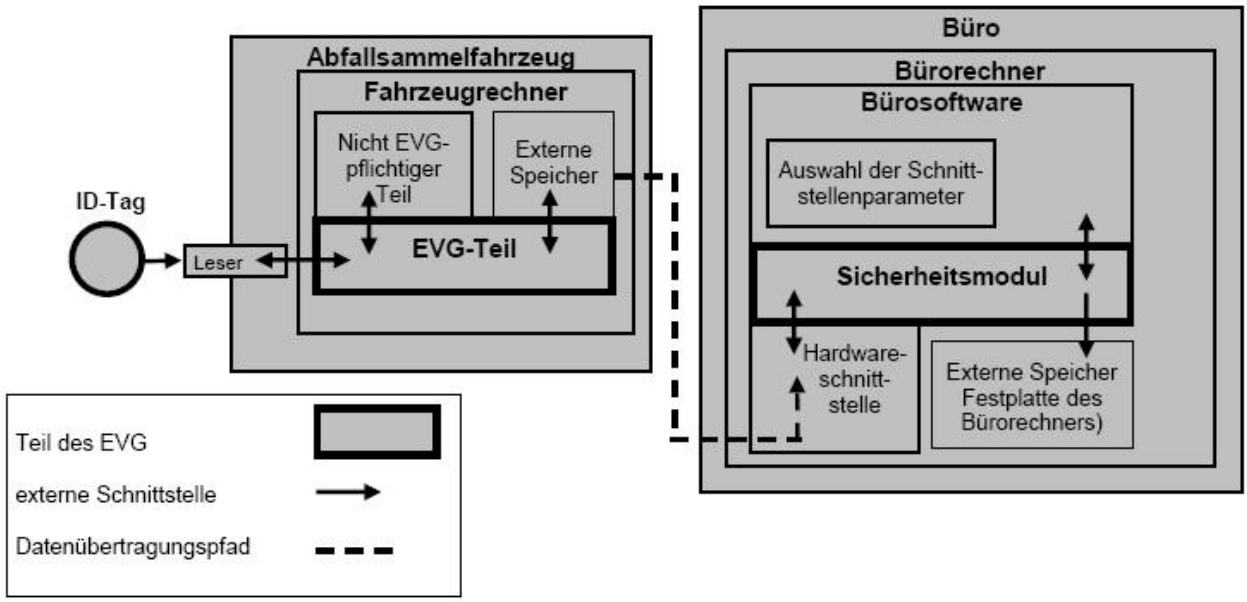

Abbildung 1: Abfallbehälter-Identifikations-System

Das System besteht aus drei getrennten Teilen. Dies sind die Transponder (ID-Tag) mit den Identifikationsdaten, das Abfallsammelfahrzeug mit dem Fahrzeugrechner und der Bürorechner mit der Bürosoftware. Der Fahrzeugrechner beinhaltet den EVG-Teil der Fahrzeugsoftware, den nicht-EVG-pflichtigen Teil der Fahrzeugsoftware und die externen Speicher, die ebenfalls nicht zum EVG gehören. Die Bürosoftware auf dem Bürorechner beinhaltet neben dem Sicherheitsmodul weitere Teile, die jedoch nicht zum EVG gehören. Des Weiteren verfügt der Bürorechner über eine Hardwareschnittstelle zur Übertragung der Leerungsdaten und einen externen Speicher zur Archivierung der gepürften Leerungsdaten. Die EVG-Teile sind in der Abbildung durch dicke schwarze Rahmen und die verschiedenen Schnittstellen der EVG-Teile durch schwarze Pfeile gekennzeichnet.

6 Dokumentation

Mit dem EVG wird folgende Dokumentation ausgeliefert:

- Gefäßidentifikationssystem Installations- und Benutzerhandbuch, Version 27/06/06 [9]
- BiDIP2 Installations- und Benutzerhandbuch, Version 27/06/06 [10]
- Handheld BHT, BHT lite, BHI, BHI Pro Manual, Version 20/09/05 [11]

Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Installation und Bedienung des EVG.

7 Testverfahren

7.1 Testkonfiguration

Das Testsystem bestand aus einer Nachbildung eines Fahrzeugsystems, einem Laptop als Testrechner, auf dem verschiedene Testsoftware zur Auswertung der Tests installiert war, einem Laptop, auf dem die Bürosoftware mit dem Sicherheitsmodul installiert wurde und verschiedenen Transpondern.

Das nachgebildete Fahrzeugsystem bestand aus folgenden Teilen:

- Box RZF134 –RZDUO, in der die Anschlüsse für Antennen und Reader zusammenlaufen
- IO-Box, an die die Simulation der Schüttungsmechanik angeschlossen wurde
- Handheld mit Cradle
- PCMCIA-Karte als Wechseldatenträger
- 2 identische BSU mit unterschiedlichen Seriennummern
- BSU-Software (EVG- und nicht-EVG-Teil)

Die Testsoftware auf dem Testrechner bestand aus

- einem Hex-Editor, mit welchem die im Binärformat vorliegenden Auszüge des Primär- bzw. Sekundärspeichers betrachtet bzw. bearbeitet werden können
- der BSI Test PC Software, einem speziell für Testzwecke erstellen, auf den Nicht-EVG-Teil der Fahrzeugsoftware abgestimmten Programm, das es erlaubt für jeden Arbeitsschritt spezielle Meldungen zu erzeugen und diese zusammen mit den Statusmeldungen des EVG-Teil anzuzeigen, sowie sektorweise auf den Primärspeicher lesend und schreibend zuzugreifen
- einem Konverter, der die vom EVG-Teil auf der Fahrzeugsoftware erzeugten Binärdateien je nach angewählter Option in ein für Menschen einfach zu lesendes Format oder in eine formatierte hexadezimale Darstellung, in welcher die Blockstrukturen einfach zu erkennen sind konvertiert
- einem Software-RFID Reader-Emulator, mit dem ein PC über die serielle Schnittstelle als RFID-Reader angesprochen werden und diesen simulieren kann
- der Update-Software, mit der die Seriennummer der BSU bestimmt, aber auch eine neue Fahrzeugsoftware in die BSU geladen werden kann

7.2 Zusammenfassung der unabhängigen Prüfstellentests

Auf Grund der geringen Anzahl von Sicherheitsanforderungen, Sicherheitsfunktionen und externen Schnittstellen entschied der Evaluator, alle Sicherheitsanforderungen, Sicherheitsfunktionen und externen Schnittstellen zu testen.

Das Gesamturteil über die durchgeführten Tests lautet „ERFÜLLT“, da in keinem Test eine deutliche Abweichung von den erwarteten Ergebnissen bzw. ein Sicherheitsrisiko basierend auf einem Fehlverhalten des EVG festgestellt werden konnte.

8 Evaluierte Konfiguration

Der EVG wird durch die Bezeichnung „**Gefäßidentifikationssystem BiTech, bestehend aus den Software-Komponenten DE_BSI_M16_LIB Version 1.5 und DE_BSI_PC_DLL Version 1.5 sowie den dazugehörigen Transpondern**“ identifiziert.

Der EVG wird lediglich in einer vor der Auslieferung festgelegten Konfiguration betrieben. Die sicherheitsrelevanten Einstellungen des EVG werden vom Hersteller vorkonfiguriert.

Das Konfigurieren der kundenzugänglichen Parameter wird in den Handbüchern [9] und [10] beschrieben.

9 Ergebnisse der Evaluierung

Der Evaluation Technical Report (ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodology [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluationsmethodology CEM [2] wurde für die Komponente aus dem Vertrauenswürdigkeitsstufe EAL 1 verwendet.

Das Urteil für die CC, Teil 3 Anforderungen an die Vertrauenswürdigkeit (gemäß EAL 1 und die Klasse ASE für die Sicherheitsvorgaben) sind in der folgenden Tabelle dargestellt.

Vertrauenswürdigkeitsklassen und Komponenten		**Urteil**
Security Target Evaluierung	CC Klasse ASE	PASS
EVG-Beschreibung	ASE_DES.1	PASS
Sicherheitsumgebung	ASE_ENV.1	PASS
ST-Einführung	ASE_INT.1	PASS
Sicherheitsziele	ASE_OBJ.1	PASS
PP-Postulate	ASE_PPC.1	PASS
IT-Sicherheitsanforderungen	ASE_REQ.1	PASS
Explizit dargelegte IT-Sicherheitsanforderungen	ASE_SRE.1	PASS
EVG-Übersichtsspezifikation	ASE_TSS.1	PASS
Konfigurationsmanagement	CC Klasse ACM	PASS
Versionsnummern	ACM_CAP.1	PASS
Auslieferung und Betrieb	CC Klasse ADO	PASS
Installation, Generierung und Anlauf	ADO_IGS.1	PASS
Entwicklung	CC Klasse ADV	PASS
Informelle funktionale Spezifikation	ADV_FSP.1	PASS
Informeller Nachweis der Übereinstimmung	ADV_RCR.1	PASS
Handbücher	CC Klasse AGD	PASS
Systemverwalterhandbuch	AGD_ADM.1	PASS
Benutzerhandbuch	AGD_USR.1	PASS
Testen	CC Klasse ATE	PASS
Unabhängiges Testen - Übereinstimmung	ATE_IND.1	PASS

Tabelle 6: Urteil zu den Vertrauenswürdigkeitskomponenten (EAL1)

Die Evaluierung hat gezeigt, dass:

- der EVG konform zum PP BSI-PP-0010-2004 [8] ist
- die Sicherheitsanforderungen für den EVG aus den Sicherheitsvorgaben Common Criteria Part 2 erweitert sind
- die Vertrauenswürdigkeit des EVG Common Criteria Teil 3 konform ist

Die Resultate der Evaluierung sind nur anwendbar auf den EVG **Gefäßidentifikationssystem BiTech** (siehe Kapitel 2 dieses Reports).

Die Gültigkeit kann auf neue Versionen bzw. Releases des Produktes erweitert werden. Voraussetzung dafür ist, dass der Antragstelle die Re-Zertifizierung oder die Assurance Continuity in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen der Sicherheitsfunktionen aufdeckt.

10 Kommentare und Empfehlungen

Die Dokumente [9] - [11] enthalten die notwendigen Informationen und Sicherheits-hinweise über die Verwendung des EVG.

11 Anhänge

keine

12 Sicherheitsvorgaben

Die Sicherheitsvorgabe [6] wird zur Veröffentlichung in einem separaten Dokument bereitgestellt.

13 Definitionen

13.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn

BSU BiTech Bus Controller

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

WBIS Waste Bin Identification System – Abfallbehälter-Identifikations-System

13.2 Glossar

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

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.

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.

14 Literaturangaben

[1] Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3, August 2005

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

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

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind

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

[6] Sicherheitsvorgaben BSI-DSZ-CC-0282-2006, Version 2.15, 27.06.2006, „Gefäßidentifikationssystem BiTech (WBIS), Sicherheitsvorgaben (ST)“, deister electronic GmbH

[7] Evaluierungsbericht, Version 1.0, 19.07.2006, „Evaluation Technical Report (ETR) BiTech“ (vertrauliches Dokument)

[8] Schutzprofil BSI-PP-0010-2004 „Protection Profile Waste Bin Identification System (WBIS-PP), Version 1.04“

[9] Gefäßidentifikationssystem Installations- und Benutzerhandbuch, Version 27/06/06

[10] BiDIP2 Installations- und Benutzerhandbuch, Version 27/06/06

[11] Handheld BHT, BHT lite, BHI, BHI Pro Manual, Version 20/09/05.

C Auszüge aus den technischen Regelwerken

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:

a) 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.

b) 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:

a) 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.

b) 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:

a) **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.

b) **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:

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

CC Part 3:

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.”

Dies ist eine eingefügte Leerseite.