Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0546-2010

zu

Gefäßidentifikationssystem Gassner GWBIS 1.50

der

GASSNER Wiege- und Messtechnik GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0546-2010

Abfallbehälter-Identifikations-System

Gefäßidentifikationssystem Gassner GWBIS 1.50

von	GASSNER Wiege- und Messtechnik GmbH
PP-Konformität:	Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, BSI-PP-0010-2004
Funktionalität:	PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

Common Criteria Recognition Arrangement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsame 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.

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.

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.

Bonn, 29. Juni 2010
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Abteilungspräsident

L.S.

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.

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

Gliederung

A Zertifizierung....7
1 Grundlagen des Zertifizierungsverfahrens....7
2 Anerkennungsvereinbarungen....7
2.1 Europäische Anerkennung von ITSEC/CC – Zertifikaten (SOGIS-MRA)....7
2.2 Internationale Anerkennung von CC – Zertifikaten (CCRA)....8
3 Durchführung der Evaluierung und Zertifizierung....8
4 Gültigkeit des Zertifikats....9
5 Veröffentlichung....9
B Zertifizierungsbericht....11
1 Zusammenfassung....12
2 Identifikation des EVG....14
3 Sicherheitspolitik....15
4 Annahmen und Klärung des Einsatzbereiches....15
5 Informationen zur Architektur....16
6 Dokumentation....17
7 Testverfahren....17
7.1 Testkonfiguration....17
7.2 Unabhängige Prüfstellentests....17
7.3 Penetrationstests....18
8 Evaluierte Konfiguration....18
9 Ergebnis der Evaluierung....19
9.1 CC spezifische Ergebnisse....19
9.2 Ergebnis der kryptographischen Bewertung....19
10 Auflagen und Hinweise zur Benutzung des EVG....19
11 Sicherheitsvorgaben....20
12 Definitionen....20
12.1 Abkürzungen....20
12.2 Glossar....21
13 Literaturangaben....22
C Auszüge aus den Kriterien....23
D Anhänge....33

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) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[5] [1]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2]
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

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.

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

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es legt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe und zusätzlich für IT-Produkte aus bestimmten technischen Bereichen auf höheren Anerkennungsstufen fest.

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen EAL1 bis EAL4 und ITSEC Vertrauenswürdigkeitsstufen E1 bis E3 (niedrig) ein. Der technische Bereich "smartcard and similar devices" wurde für

---

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

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 Informati-onstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

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

höhere Anerkennungsstufen definiert. Er schließt Vertrauenswürdigkeitsstufen oberhalb von EAL4 bzw. E3 (niedrig) ein.

Das neue Abkommen wurde zu Beginn von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Niederlande, Norwegen, Schweden und Spanien unterzeichnet.

Im Rahmen dieses Abkommens erkennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) an:

- für die Basisanerkennungsstufe die Zertifikate von Großbritannien, Frankreich, Niederlande und Spanien, die ab April 2010 erteilt wurden.
- für höhere Anerkennungsstufen die Zertifikate für Produkte aus dem Bereich "smartcard and similar devices" von Großbritannien, Frankreich und den Niederlanden, die ab April 2010 erteilt wurden.

Zusätzlich ist die Anerkennung von Zertifikaten, die für Common Criteria Schutzprofile erteilt werden, Bestandteil des Abkommens.

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

Das erste SOGIS-Anerkennungsabkommen Version 1 (nur ITSEC) trat im März 1998 in Kraft. Es wurde im Jahre 1999 auf Zertifikate nach Common Criteria erweitert (MRA Version 2). Zertifikate, die unter diesen älteren Versionen des Abkommen erteilt wurden, sind weiterhin anerkannt.

2.2 Internationale Anerkennung von CC – Zertifikaten (CCRA)

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 verabschiedet (CC-MRA).

Der Vereinbarung sind bis Januar 2009 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, 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 Common Criteria-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

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 Gassner GWBIS 1.50 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Gefäßidentifikationssystem Gassner GWBIS 1.50 wurde von atsec information security GmbH durchgeführt. Die Evaluierung wurde am 22. April 2010

beendet. Das Prüflabor atsec information security GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: GASSNER Wiege- und Messtechnik GmbH

Das Produkt wurde entwickelt von: GASSNER Wiege- und Messtechnik GmbH

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

4 Gültigkeit des Zertifikats

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

Das Produkt ist nur unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitsstufen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports erläutert.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiterentwickelten Methoden in Zukunft möglich sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance Continuity-Programms des BSI regelmäßig überprüfen zu lassen. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt 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.

5 Veröffentlichung

Das Produkt Gefäßidentifikationssystem Gassner GWBIS 1.50 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[7]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

---

[6] Information Technology Security Evaluation Facility

[7] GASSNER Wiege- und Messtechnik GmbH
Münchner Bundesstraße 123
A-5020 Salzburg
Österreich

Dies ist eine eingefügte Leerseite.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

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

1 Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist das Gefäßidentifikationssystem Gassner (GWBIS), Version 1.50.

Das Gefäßidentifikationssystem dient der verursacherbezogenen Abrechnung und Veranlagung der Gebühren der Abfallwirtschaft. Das System kann außer im kommunalen Einsatz zur Gebührenveranlagung auch im privaten und gewerblichen Bereich eingesetzt werden.

Das System bietet die Möglichkeit, die Abrechnung über die Anzahl der Leerungen eines Abfallbehälters durchzuführen. Das System kann optional z.B. ein Wiege- oder Volumenmesssystem enthalten, um auch zur gewichtsbezogenen Abrechnung benutzt zu werden.

Die Abfallbehälter werden mit einem Datenträger (ID-Tag) ausgestattet. Der ID-Tag speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Leser ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden von der Fahrzeugsoftware erkannt. Die Identifizierungsdaten werden dann an die Fahrzeugsoftware weitergeleitet. Optional wird das Gewicht der Abfälle oder der Füllstand der Tonne durch eine entsprechende Sensorik im Fahrzeug ermittelt und parallel zu den Identifizierungsdaten an die Fahrzeugsoftware übermittelt.

Die Fahrzeugsoftware ergänzt diese Daten um Datum- und Zeitangaben, bildet daraus einen Leerungsdatensatz und speichert diese redundant. Die Leerungsdatensätze werden in Leerungsdatenblöcken vom Fahrzeugrechner über das Sicherheitsmodul an die Bürosoftware übermittelt. Die Fahrzeugsoftware sorgt durch geeignete Maßnahmen (z.B. Backup der Daten) dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist. Bei der Übermittlung der Leerungsdatenblöcke an die Bürosoftware wird durch das Sicherheitsmodul sichergestellt, dass nur die in einem registrierten Fahrzeug erstellten Leerungsdatensätze als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler oder Manipulationen erkannt.

Nach der Prüfung der übertragenen Daten durch das Sicherheitsmodul können diese Daten an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, BSI-PP-0010-2004 [8].

Die Vertrauenswürdigkeitskomponenten (Security Assurance Requirements SAR) sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 6.1 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als CC Teil 2 erweitert.

Die funktionalen Sicherheitsanforderungen werden durch die folgenden Sicherheitsfunktionen des EVG umgesetzt:

Sicherheitsfunktion des EVG	Thema
TSF_IDCHK	Prüfung der Identifikationsdaten
TSF_GFE-KEN	Generierung eines Gültigkeitsmerkmals für Leerungsdatensätze
TSF_AT+CRC	Generierung eines Integritätsmerkmals für Leerungsdatensätze und Leerungsdatenblöcke
TSF_SAFE	Redundante Speicherung
TSF_GFE-CHK	Gültigkeitsprüfung der Leerungsdatensätze
TSF_AT+CHK	Integritätsprüfung der Leerungsdatensätze und Leerungsdatenblöcke

Tabelle 1: Sicherheitsfunktionen des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 7.1 dargestellt.

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 4.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in den Kapiteln 4.2 – 4.4 dar.

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 Evaluierungsgegenstand (EVG) heisst:

Gefäßidentifikationssystem Gassner GWBIS 1.50

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr.	Typ	Bezeichnung	Version	Auslieferungsart
1	HW	Stifttransponder	Envicomp TI-134 2Khz-HDX-R/O-Wedge	
		23mm Glastransponder	Texas Instruments RI-TRPREHP- 30	
		32mm Glastransponder	Texas Instruments RI-TRPRE2B- 30	
		120mm Kunststoffrohr	Texas Instruments RI-TRPR9TD- 16	
		Schlüsselanhänger	Texas Instruments RI-TRP-RFoB	
2	SW	Firmware in der Fahrzeugeinheit	SWE-BLK-1.01 (für Balkenschütte) SWE-DS-1.01 (für Doppelschütte)	Wird durch den Hersteller auf dem Fahrzeugrechner installiert
3	DOC	Installationshandbuch	Handbuch_Junior.pdf: Juni 2007 [10]	Papierausdruck
4	DOC	Benutzerhandbuch	User.pdf: Juni 2009 [11]	Papierausdruck
5	SW	Sicherheitsmodul	Communicator.exe, Version 1.6.0.1	Wird durch den Hersteller auf dem Bürorechner installiert
6	DOC	Installations- und Benutzerhandbuch Communicator	Version 1.6.0.1, letzte Änderung: 25.03.2010 [12]	Papierausdruck

Tabelle 2: Auslieferungsumfang des EVG

Der EVG wird ausschließlich durch Servicepersonal des Herstellers ausgeliefert, installiert und konfiguriert.

3 Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionen des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte:

- Erzeugung eines Gültigkeitsmerkmals für die Leerungsdaten
- Manipulationsschutz der Leerungsdaten bei der Übertragung
- Integritätsschutz der gespeicherten Daten
- Redundante Speicherung
- Erkennung einer Übermittlung willkürlicher (z. B. ungültiger) Leerungsdatenblöcke an das Sicherheitsmodul

4 Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind die folgenden Punkte relevant:

- Montage der Transponder (ID-Tags)
- Vertrauenswürdiges Personal
- Zugangsschutz zum EVG
- Überprüfung der vollständigen Übertragung der Leerungsdatenblöcke
- Datensicherung
- Systeminstallation

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 5.2.

5 Informationen zur Architektur

Das Abfallbehälter-Identifikations-System besteht aus folgenden Komponenten:

- ID-Tag mit den Identifizierungsdaten des Abfallbehälters.
- Fahrzeug mit dem (ID-Tag-) Reader, Fahrzeugrechner und einem optionalen Wiege-, Volumenmess- oder ähnlichem System. Die Fahrzeugsoftware ist installiert auf dem Fahrzeugrechner. Der Fahrzeugrechner, an dem auch die genannten optionalen Komponenten angeschlossen werden können und auf dem die Fahrzeugsoftware installiert ist, wird als Gassner Fahrzeug Einheit bezeichnet.
- Bürorechner im Büro. Das Sicherheitsmodul und die Bürosoftware auf dem Bürorechner sind installiert.

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

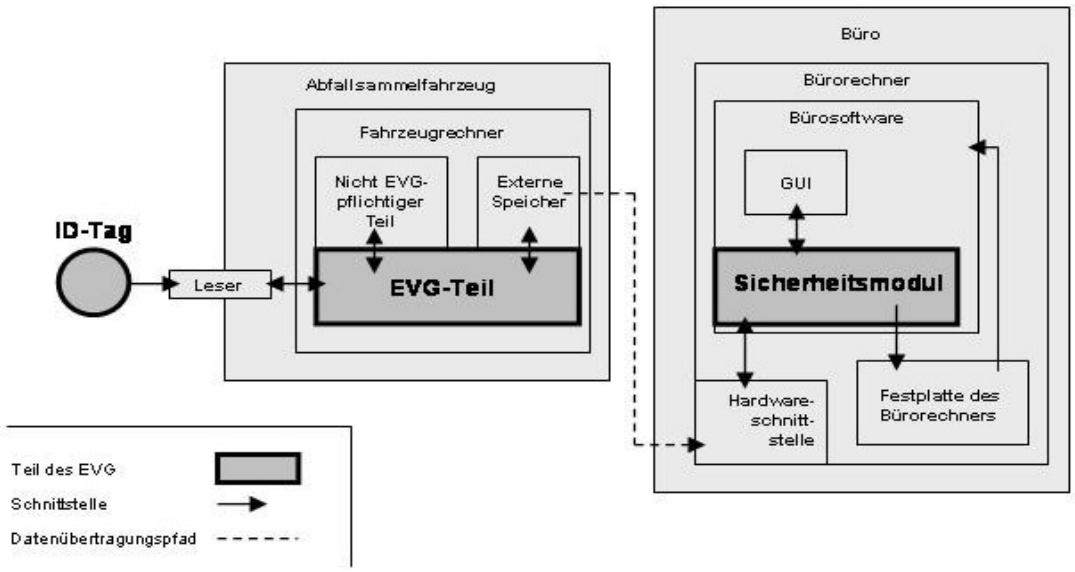

Abbildung 1: Abfallbehälter-Identifikations-System

Das System besteht aus drei getrennten Teilen. Dies sind die Transponder (ID-Tags) mit den Identifikationsdaten, das Abfallsammelfahrzeug mit dem ID-Tag Reader und dem Fahrzeug-Rechner sowie der Bürorechner mit dem Sicherheitsmodul und der Bürosoftware. Der Fahrzeugrechner beinhaltet die Fahrzeugsoftware. Sie besteht aus dem EVG-Teil der Fahrzeugsoftware (SWE-BLK-1.01 (für Balkenschütte), SWE-DS-1.01 (für Doppelschütte)) und dem nicht zum EVG gehörenden Teil der Fahrzeugsoftware. Im Fahrzeugrechner befindet sich außerdem ein externer Speicher zur redundanten Speicherung der Leerungsdatensätze. Der Bürorechner beinhaltet als Teil der Bürosoftware das zum EVG gehörige Sicherheitsmodul Communicator.exe, Version 1.6.0.1 und eine Benutzerschnittstelle (GUI). Des Weiteren verfügt der Bürorechner über eine Hardwareschnittstelle zur Übertragung der Leerungsdaten vom Fahrzeugrechner an das Sicherheitsmodul und eine Festplatte. Die EVG-Teile sind in der Abbildung fett umrandet und die verschiedenen Schnittstellen durch schwarze Pfeile gekennzeichnet.

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7 Testverfahren

7.1 Testkonfiguration

Die unabhängigen Tests des Evaluators wurden auf beiden erlaubten Hardwarekonfigurationen durchgeführt, d.h. es wurde der Bordrechner DMA02 Junior mit jeweils simulierter Balken- bzw. Doppelschütte und zugehöriger Firmware SWE-BLK-1.01 bzw. SWE-DS-1.01 getestet. Die beiden erlaubten Waagenkonfigurationen unterscheiden sich lediglich hinsichtlich der mechanischen Kopplung der Waagen; die Sicherheitsfunktionalität des EVG ist für beide Konfigurationen identisch.

Die Pentrationstests wurden nur auf einer der beiden erlaubten Hardwarekonfigurationen durchgeführt, d.h. es wurde der Bordrechner DMA02 Junior mit simulierter Balkenschütte und zugehöriger Firmware SWE-BLK-1.01 getestet.

Für die Tests wurden vier Transponder vom Typ RI-TRP-RE2B-30 verwendet, d.h. Glastransponder mit einer Länge von 32mm verbaut in einem runden Plastikgehäuse. Für alle übrigen laut Sicherheitsvorgaben für die Verwendung mit dem EVG zugelassenen Transpondertypen wurden vom Hersteller Muster zur Verfügung gestellt, welche erfolgreich hinsichtlich ihrer korrekten Erkennung durch den EVG geprüft wurden. Alle vom Hersteller bereitgestellten Transponder waren mit einer eindeutigen ID versehen.

Das Sicherheitsmodul wurde in seiner evaluierten Version, d.h. Version 1.6.0.1, verwendet.

Vor Beginn der Tests hat der Evaluator die Korrektheit der Versionsstände von Bordrechner und Sicherheitsmodul überprüft.

7.2 Unabhängige Prüfstellentests

Der vom Evaluator gewählte Testansatz betrachtete alle externen Schnittstellen des EVG, d.h. auch solche, welche nicht unmittelbar über die Benutzerschnittstellen am Bordrechner oder am Sicherheitsmodul ereichbar sind.

Um die korrekte Funktion des EVG zu testen, erarbeitete der Evaluator Testfälle, die den Weg einer Transponder-ID vom Transponder zur Bürosoftware nachverfolgen und den Schutz der Gültigkeit und Integrität der übertragenen Datensätze prüfen. Hierbei hat der Evaluator versucht, durch gezielte Angriffe auf den EVG rein zufällige Veränderungen, wie in den Sicherheitsvorgaben als Bedrohung beschrieben, herbeizuführen bzw. hat verifiziert, dass manuelle Änderungen vom EVG zuverlässig erkannt und gemeldet werden.

Die Tests haben keine signifikanten Abweichungen der tatsächlichen Testergebnisse von den erwarteten Ergebnissen gezeigt. Alle Abweichungen konnten vom Evaluator als konform zu den erwarteten Ergebnissen verifiziert werden.

7.3 Penetrationstests

Der Evaluator hat zunächst eine Internetrecherche zu produktspezifischen Schwachstellen des EVG durchgeführt, welche jedoch keine offensichtlichen Schwachstellen offenbarte.

Im Anschluss daran hat der Evaluator anhand der in den Sicherheitsvorgaben beschriebenen Bedrohungen mögliche Angriffsszenarien ermittelt und hinsichtlich ihrer Ausnutzbarkeit analysiert. Dabei hat er festgestellt, dass es neben für den EVG irrelevanten Schwachstellen auch solche gibt, für die ein Angreifer ein Angriffspotenzial jenseits von "Basic" benötigt. Zudem hat der Evaluator eine mögliche Schwachstelle identifzieren können, für deren Ausnutzung keine zusätzlichen Werkzeuge oder Fachkenntnisse benötigt werden. Durch einen entsprechenden Penetrationstest konnte der Evaluator jedoch nachweisen, dass der EVG dieser Schwachstelle erfolgreich entgegenwirkt und somit der EVG resistent gegen Angrifsszenarien ist, die ein Angriffspotenzial von "Basic" voraussetzen.

Die Tests haben keine Abweichung der tatsächlichen Testergebnisse von den erwarteten Ergebnissen gezeigt. Der durchgeführte Penetrationsversuch war nicht erfolgreich, d.h. der EVG ist in seiner operativen Umgebung resistent gegen Angriffe von Angreifern mit Angriffspotenzial "Basic", sofern alle in den Sicherheitsvorgaben geforderten Maßnahmen umgesetzt sind.

8 Evaluierte Konfiguration

Der EVG wird durch die Bezeichnung Gefäßidentifikationssystem Gassner (GWBIS), Version 1.50, bestehend aus der Firmware der Fahrzeugeinheit (SWE-BLK-1.01 (für Balkenschütte), SWE-DS-1.01 (für Doppelschütte)) und dem Sicherheitsmodul (Communicator.exe, Version 1.6.0.1) sowie den Transpondern (ID-Tags) laut Nummer 1 in Tabelle 2 identifiziert.

Der EVG kann in zwei Konfigurationen betrieben werden. Die Konfigurationen unterscheiden sich lediglich in der Version der Firmware der Fahrzeugeinheit. Diese berücksichtigen die beiden erlaubten Waagenkonfigurationen, die sich lediglich hinsichtlich der mechanischen Kopplung der Waagen unterscheiden; die Sicherheitsfunktionalität des EVG ist für beide Konfigurationen identisch.

Dieses Zertifikat bezieht sich ausschließlich auf diese Konfigurationen des EVG.

Nur die in Tabelle 2 aufgeführten Transpondertypen gehören zum EVG und dürfen verwendet werden.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [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. Die Evaluierungsmethodologie CEM [2] wurde für die Komponenten bis zur Vertrauenswürdigkeitsstufe EAL 1 verwendet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeits-komponenten bestätigt:

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 1 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die Komponenten
  ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

Die Evaluierung hat gezeigt:

- PP Konformität: Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, BSI-PP-0010-2004 [8]
- Funktionalität: PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2 Ergebnis der kryptographischen Bewertung

Der EVG enthält keine kryptografischen Algorithmen. Daher wurden auch keine solchen Mechanismen bewertet.

10 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind alle Aspekte der Annahmen, Bedrohungen und Politiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.

Zusätzlich sind die folgen Auflagen und Hinweise zu beachten:

- Nur die in Tabelle 2 aufgeführten Transpondertypen gehören zum EVG und dürfen verwendet werden.

11 Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12 Definitionen

12.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn

BSIG BSI-Gesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

CEM Common Methodology for Information Technology Security Evaluation – Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluierungsgegenstand

GUI Graphical User Interface - Benutzerschnittstelle

IT Information technology - Informationstechnologie

ITSEF Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit

PP Protection Profile – Schutzprofil

SAR Security Assurance Requirement – Vertrauenswürdigkeitsanforderung

SFP Security Function Policy – Funktionale Sicherheitspolitik

SFR Security Functional Requirement – Funktionale Sicherheitsanforderung

ST Security Target – Sicherheitsvorgaben

TOE Target of Evaluation – Evaluierungsgegenstand

TSF TOE Security Functionality - EVG-Sicherheitsfunktionalität

12.2 Glossar

Anmerkung: In den folgenden Begriffsdefinitionen werden zu den deutschen Begriffen jeweils die englische Übersetzung und die englische Definition geliefert, da keine vollständige aktuelle Übersetzung der Common Criteria Version 3.1 vorliegt.

Erweiterung - Extension
The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Evaluierungsgegenstand - Target of Evaluation
A set of software, firmware and/or hardware possibly accompanied by guidance.

EVG-Sicherheitsfunktionalität - TOE Security Functionality
The combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

Formal – Formal
Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Funktionale Sicherheitspolitik – Security Function Policy
A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

Informell - Informal
Expressed in natural language.

Objekt - Object
A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Schutzprofil - Protection Profile
An implementation-independent statement of security needs for a TOE type.

Sicherheitsvorgaben - Security Target
An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Semiformal
Expressed in a restricted syntax language with defined semantics.

Subjekt - Subject
An active entity in the TOE that performs operations on objects.

Zusatz - Augmentation
The addition of one or more requirement(s) to a package.

13 Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1, Revision 2, September 2007

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1, Revision 2, September 2007

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

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind [8]

[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-0546-2010, Version 2.0, 25.03.2010, „Gefäßidentifikationssystem Gassner (GWBIS) Version V-GWBIS-1.50 Sicherheitsvorgaben (ST)“, GASSNER Wiege und Messtechnik GmbH

[7] Evaluierungsbericht, Version 2, 22.04.2010, „Final ETR“, atsec information security GmbH (vertrauliches Dokument)

[8] Protection Profile Waste Bin Identification Systems (WBIS-PP), BSI-PP-0010-2004 Version 1.04, 27.05.2004, Deutscher Städte- und Gemeindebund

[9] Konfigurationsliste für GWBIS 1.50 vom 22.04.2010 (vertrauliches Dokument)

[10] Technisches Handbuch Wägeterminal DMA 02 junior, Juni 2007, GASSNER Wiege und Messtechnik GmbH

[11] Bedienungsanleitung Wägeterminal DMA 02 junior, Juni 2009, GASSNER Wiege und Messtechnik GmbH

[12] “Communicator Version 1.6.0.1 Dokumentation”, 25.03.2010, GASSNER Wiege und Messtechnik GmbH

[8] Inbesondere:

- AIS 32, Version 5, 17. Mai 2010, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1, Revision 2 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in

which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.”

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

Dies ist eine eingefügte Leerseite.

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben [6] werden in einem eigenen Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.