Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0618-2011

zu

Envicomp Security System ESS Version 3.0

der

Envicomp Systemlogistik 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-0618-2011

Abfallbehälter-Identifikations-System

Envicomp Security System ESS
Version 3.0

von	Envicomp Systemlogistik GmbH
PP-Konformität:	Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, BSI-PP-0010-2004
Funktionalität:	PP konform 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 Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert.

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, 09. Mai 2011

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski L.S.
Abteilungspräsident

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

Dies ist eine eingefügte Leerseite.

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

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 Informationstechnik (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

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 Envicomp Security System ESS, Version 3.0, hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Envicomp Security System ESS, Version 3.0, wurde von T-Systems GEI GmbH durchgeführt. Die Evaluierung wurde am 23. März 2011 beendet. Das Prüflabor T-Systems GEI GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: Envicomp Systemlogistik GmbH

Das Produkt wurde entwickelt von: Envicomp Systemlogistik 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 und die Stärke der Funktionen 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 sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

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.

---

[6] Information Technology Security Evaluation Facility

5 Veröffentlichung

Das Produkt Envicomp Security System ESS, Version 3.0 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.

[7] Envicomp Systemlogistik GmbH
Bünder Strasse 85
32051 Herford

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.

1 Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist das „Envicomp Security System, Version 3.0 (ESS)“ (im weiteren „ESS 3.0“ genannt), ein sogenanntes „Waste Bin Identification System (WBIS)“ oder Abfallbehälter-Identifikationssystem.
Es besteht aus den Transpondern (ID-Tags), den ID-Tag-Readern, dem Fahrzeugrechner IO03 und dem Sicherheitsmodul EnviCONVERT (siehe auch Tabelle 2 und Kapitel 8).

Die Abfallbehälter werden mit einem 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 der Leerung eines Abfallbehälters durch den Leser ausgelesen. Mögliche Übertragungsfehler und eventuelle Manipulationen werden vom Leser 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 diesen redundant im Primär- und Sekundärspeicher. 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 Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, BSI-PP-0010-2004 [7]. Die Anforderungen des WBIS-PP werden vollständig erfüllt.

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 5.1 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 folgende Sicherheitsfunktionalität des EVG umgesetzt:

Sicherheitsfunktionalität des EVG	Thema
FDP_DAU.1.1	Erzeugung einer Gültigkeitsgarantie
FDP_DAU.1.2	Verifizierung einer Gültigkeitsgarantie
FDP_ITT.5.1	Integrität der internen Übertragung
FDP_SDI.1.1	Überwachung der Integrität der gespeicherten Daten
FRU_FLT.1.1	Datensicherung

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 5.2 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3.3 – 3.5 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:

Envicomp Security System ESS, Version 3.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Bezeichnung	Release	Datum	Auslieferungsname	Übergabeform
1	Dok	Handbuch „Technischer Benutzer“	V1.0	14.05.09	0090009 Technischer Benutzer Handbuch	Handbuch
2	Dok	EnviCONVERT Dokumentation	V2.1	12.07.10	0090009 EnviCONVERT Dokumentation	Handbuch
3	Dok	Handlungs-anweisungen	V2.0	06.05.10	0090009 Handlungsanweisungen	Dokument
4	Dok	Handbuch BC04	V1.0	25.05.09	0090009 Handbuch BC04	Handbuch
5	SW	EnviCONVERT	V1.00.3510. 17478	09.07.09	EnviCONVERT Secure V1.0	CD-ROM
6	HW	ID-Tag	siehe ST [6], Kapitel 5.14, Tag-Varianten	01.03.09	SAP gemäß ST [6], Kapitel 5.14, Tag-Varianten	Hardware
7	HW	IO03	V3.0	01.03.09	IO03	Hardware
7.1	SW	Controller SW IO03	455510_0001 _0020.bin	09.07.09	455510_0001_0020.bin	Software
8	HW	Reader Multireader	SR 13401 / SR 13402	01.03.09	Multireader SR 13401 / SR 13402	Hardware
8.1	SW	Reader SW	SR_705m.bin	-	705m	Software
9	HW	Reader Tiris	Series 2000	-	TI-Reader	Hardware
9.1	SW	Reader SW	1.50.bin	-	1.50	Software
10	HW	Reader Tagsys	P013	-	P013 Reader	Hardware
10.1	SW	Reader SW	LF11776V2.1	-	V1.6	Software
11	HW	Mikron-Reader (HF-Teil)	RWDDHFE1 M1100019	-	HF-Teil	Hardware

Tabelle 2: Auslieferungsumfang des EVG

Die Fahrzeugausstattung einschließlich des EVGs wird betriebsfertig vom Hersteller installiert und ausgeliefert.

Darüber hinaus bestehen folgende Identifizierungsmöglichkeiten:

Die ID-Tags können durch die Angabe der SAP-Artikelnummer als EVG-Bestandteil identifiziert werden (siehe ST [6], Kapitel 5.14).

Der IO03 erhält einen Aufkleber als Typenschild. Das Typenschild enthält die Bezeichnung der Hardware "IO03 V 3.0" und identifiziert die Controllersoftware als "455510_0001_0020.bin".

Die Reader erhalten jeweils auch einen Aufkleber als Typenschild.

Der Multireader wird durch die Angabe "SR 13401" oder „SR 13402“ identifiziert.

Der TI-Reader wird durch die Angaben "TI-Reader Series 2000" und die Softwareversion "1.50" identifiziert.

Der Tagsys Reader wird durch die Angaben "P013 Reader" und die Version "1.6" der Reader-Software identifiziert.

Der Mikron-Reader wird im IO03 verbaut. Das Typenschild des IO03 zeigt die zugehörigen Angaben: "Mikron-Reader HF-Teil" und "RWDDHFE1M1100019".

Das Sicherheitsmodul EnviCONVERT kann nach der Installation durch die Angabe der Versionsnummer 1.0.3510.17478 in einem Informationsfenster der Software identifiziert werden.

3 Sicherheitspolitik

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

- Erzeugung einer Gültigkeitsgarantie für Leerungsdatensätze AT und Leerungsdatenblöcke AT+
- Verifizierung dieser Gültigkeitsgarantien
- Integrität der internen Übertragung zwischen physisch getrennten Teilen des EVG
- Überwachung der Integrität der gespeicherten Daten (Identifizierungsdaten AT1 im ID-Tag und Leerungsdatensätze AT während der Speicherung im Sammelfahrzeug)
- Redundante Datenspeicherung

4 Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind insbesondere die folgenden Punkte relevant:

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

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5 Informationen zur Architektur

Der EVG besteht aus mehreren verteilten Komponenten, den ID-Tags zur Identifizierung von Abfallbehältern, dem Fahrzeugrechner zur Erfassung und Speicherung der Leerungsdaten und der Software EnviCONVERT zur Prüfung und Darstellung der Leerungsdaten.

Die ID-Tags sind an den Abfallbehältern fest angebracht. Vor oder während der Leerung liest die Fahrzeugausstattung die in einem ID-Tag gespeicherten Daten und erzeugt daraus zusammen mit weiteren Daten den Leerungsdatensatz AT, der von der Fahrzeugausstattung gespeichert wird. Die Fahrzeugausstattung bildet aus mehreren Leerungsdatensätzen AT einen Leerungsdatenblock AT+. Leerungsdatenblöcke AT+ werden mithilfe eines USB-Sticks oder mittels GPRS an einen Arbeitsplatz-PC übertragen. Weder der USB-Stick noch die GPRS-Übertragungseinrichtungen gehören zum EVG.

Die Software EnviCONVERT ist auf einem Arbeitsplatz-PC installiert und dient der Prüfung und Darstellung der Leerungsdatensätze AT und Leerungsdatenblöcke AT+. Die geprüften Leerungsdaten werden verwendet, um beispielsweise Abrechnungen für die stattgefundenen Entsorgungen zu erstellen.

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.

7 Testverfahren

7.1 Testkonfiguration

Die Tests wurden mit zwei unterschiedlichen Konfigurationen durchgeführt.

Testkonfiguration 1 bestand aus den ID-Tags 4101256 und 4101248, dem Reader P013 (mit Software-Version LF11776V2.1), dem Fahrzeugrechner IO03 (Version V3.0 01.03.2009) und dem Sicherheitsmodul EnviCONVERT (Version 1.0.3510.17).

Testkonfiguration 2 bestand aus allen im ST [6] in Kapitel 5.14 gelisteten ID-Tags, den drei Readern Envicomp Multi-Reader SR13401 (mit Software-Version 705m), TI-Reader S2000 (mit Software-Version 1.50) und Tagsys Reader P013 (mit Software-Version 1.6), dem Fahrzeugrechner IO03 (Version V3.0 01.03.2009) sowie dem Sicherheitsmodul EnviCONVERT (Version 1.0.3510.17478).

7.2 Unabhängige Evaluatortests

Die durchgeführten Tests deckten bis auf die Schnittstelle zwischen Reader und Fahrzeugrechner alle Schnittstellen ab. Die Tests deckten die komplette Sicherheitsfunktionalität ab. Hierzu wurde der komplette Weg der Identifizierungsdaten auf den ID-Tags bis zur Überprüfung der Leerungsdaten im Sicherheitsmodul nachgebildet. Die Tests haben keine Abweichungen der tatsächlichen Testergebnisse von den erwarteten Ergebnissen gezeigt. Die Sicherheitsfunktionalität wirkt wie beschrieben.

7.3 Penetrationstests

Während der Evaluierung wurden öffentlich verfügbare Informationen benutzt (Internet, CERT-Dienst, Fachpublikationen), um produktspezifische Schwachstellen zu identifizieren. Dabei wurde festgestellt, dass keine offensichtlichen Schwachstellen bekannt sind.

Während der Evaluierung wurden, ausgehend von den Bedrohungen aus den Sicherheitsvorgaben, potentielle Angriffsszenarien identifiziert und analysiert, ob sie ausnutzbar sind. Die Analyse zeigte, dass es relevante Schwachstellen gibt, für die ein Angreifer ein Angriffspotenzial von mindestens "Moderate" benötigt. Durch Penetrationstests hat der Evaluator nachgewiesen, dass der EVG in seiner operativen Einsatzumgebung diesen Schwachstellen erfolgreich entgegenwirkt. Der EVG widersteht daher mindestens Angriffen mit einem Angriffspotenzial entsprechend der Stufe "Basic".

8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

- ID-Tags: alle im ST [6], Kapitel 5.14 genannten ID-Tags (identifiziert durch die jeweilige SAP-Artikelnummer)
- ID-Tag-Reader: Envicomp Multi-Reader SR 13401 / SR 13402 (mit Software-Version 705m), TI-Reader S2000 (mit Software-Version 1.50), Tagsys Reader P013 (mit Software-Version 1.6), Mikron-Reader HF-Teil (mit Software-Version RWDDHFE1 M1100019)
- Fahrzeugrechner IO03 (Version 3.0, 01.03.09)
- Sicherheitsmodul EnviCONVERT (Version 1.0.3510.17478)

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [8] 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.

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 [7]
- Funktionalität: PP konform
  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.

11 Sicherheitsvorgaben

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

12 Definitionen

12.1 Abkürzungen

AIS Anwendungshinweise und Interpretationen zum Schema

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

BSIG BSI-Gesetz

CCRA Common Criteria Recognition Arrangement

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

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

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

ETR Evaluation Technical Report

EVG Evaluierungsgegenstand (EVG)

IT Information technology - Informationstechnologie

ITSEC Information Technology Security Evaluation Criteria

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

PP Protection Profile - Schutzprofil

SAR Security Assurance Requirement - Vertrauenswürdigkeitsanforderung

SFP Security Function Policy – Politik der Sicherheitsfunktion

SFR Security Functional Requirement – Funktionale Sicherheitsanforderungen

ST Security Target – Sicherheitsvorgaben

TOE Target of Evaluation –Evaluierungsgegenstand

TSF TOE Security Functionality - EVG-Sicherheitsfunktionalität

12.2 Glossar

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

Evaluationsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher.

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

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

Informell - Ausgedrückt in natürlicher Sprache.

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

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

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

Sicherheitsvorgaben - Eine implementierungsabhängige Menge von Sicherheits-anforderungen für eine Kategorie von EVG.

Subjekt – Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

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

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

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

[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), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird

[6] Sicherheitsvorgaben BSI-DSZ-0618-2011, Version 3.2, 10.01.2011, Sicherheitsvorgaben ESS 3.0, Envicomp Systemlogistik GmbH

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

[8] Evaluierungsbericht, Version 1.04, 18.03.2011, T-Systems GEI GmbH (vertrauliches Dokument)

[9] Konfigurationsliste für den EVG, Version 3.4, 11.01.2011, Konfigurationsliste Envicomp Security System ESS, Version 3.0, Envicomp Systemlogistik GmbH (confidential document)

[10] Envicomp Security System ESS, Version 3.0, Handbuch Technischer Benutzer, Version 1.0, 14.05.2009; Envicomp Systemlogistik GmbH

[11] Envicomp Security System ESS, Version 3.0, EnviCONVERT Dokumentation, Version 2.1, 12.07.2010; Envicomp Systemlogistik GmbH

[12] Envicomp Security System ESS, Version 3.0, Handlungsanweisungen, Version 2.0, 06.05.2010, Envicomp Systemlogistik GmbH

[13] Envicomp Security System ESS, Version 3.0, Handbuch BC04, Version 1.0, 25.05.2009, Envicomp Systemlogistik GmbH

[8] Inbesondere:

- AIS 32, Version 6, 3. August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

Dies ist eine eingefügte Leerseite.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 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 werden in einem eigenen Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.