Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0496-2008

zu

MAWIS Rev. 3.0

der

MOBA Mobile Automation AG

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0496-2008

Abfallbehälter-Identifikations-System

MAWIS Rev. 3.0

von	MOBA Mobile Automation AG
PP-Konformität:	Protection Profile Waste Bin Identification System (WBIS-PP) Version 1.04 BSI-PP-0010-2004
Funktionalität:	PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 konform
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 1

Common Criteria Arrangement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) 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, 16. Mai 2008

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

IT Security Certified

SOGIS - MRA

Joachim Weber
Fachbereichsleiter

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

Dies ist eine eingefügte Leerseite.

Vorbemerkung

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

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

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

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

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

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

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

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG[2]
- BSI-Zertifizierungsverordnung [3]
- BSI-Kostenverordnung [4]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Hinweise der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

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

[3] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7.Juli 1992, Bundesgesetzblatt I S. 1230

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

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

2.1 Europäische Anerkennung von ITSEC/CC - Zertifikaten

Ein Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf deren Grundlage ITSEC-Zertifikate für IT-Produkte unter gewissen Bedingungen anerkannt werden, ist im März 1998 in Kraft getreten (SOGIS-MRA).

Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien im Rahmen dieses Abkommens an.

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

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 Februar 2007 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn, USA.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungstellen 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 MAWIS Rev. 3.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts MAWIS Rev. 3.0 wurde von der Tele-Consulting security / networking / training GmbH durchgeführt. Die Evaluierung wurde am

29. April 2008 beendet. Das Prüflabor Tele-Consulting security / networking / training GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: MOBA Mobile Automation AG.

Das Produkt wurde entwickelt von: MOBA Mobile Automation AG.

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 des Einsatzes 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 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.

[6] Information Technology Security Evaluation Facility

5 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-12 und D1 bis D-2.

Das Produkt MAWIS Rev. 3.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[7] MOBA Mobile Automation AG
Niederlassung Dresden
Freibergstr. 69 – 71
01159 Dresden

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

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

Gliederung des Zertifizierungsberichtes

1 Zusammenfassung

Beim EVG handelt es sich um das Abfallbehälter-Identifikationssystem MAWIS Rev. 3.0, bestehend aus der Sicherheitskomponente der Fahrzeugsoftware MAWISMobilSecurity.dll, Version 1.0.812.1 und dem Sicherheitsmodul MawisSecurity.exe, Version 1.0.808.1 sowie den Transpondern (ID-Tags) mit den MOBA-Artikel-Nummern 02-21-00000 bis 02-21-02000.

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

Die Vertrauenswürdigkeitskomponenten sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 1.

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 Teil 2 erweitert.

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

Sicherheitsfunktion des EVG	**Thema**
TSF_Crc_ccittv	Prüfung der Identifikationsdaten
TSF_GenerateAT_Check	Generierung eines Gültigkeitsmerkmals für Leerungsdatensätze
TSF_GenerateATPlus_Check	Generierung eines Gültigkeitsmerkmals für Leerungsdatenblöcke
TSF_Store_ATPlus	Redundante Speicherung
TSF_Check_ATPlus	Gültigkeits- und Integritätsprüfung der Leerungsdatenblöcke im Sicherheitsmodul
TSF_Check_AT	Gültigkeits- und Integritätsprüfung der Leerungsdatensätze im Sicherheitsmodul

Tabelle 1: Sicherheitsfunktionen des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

Die Werte, die durch den TOE 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 3.1 bis 3.3 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:

MAWIS Rev. 3.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Bezeichnung	Version	Auslieferungsart
1	HW	ID-Tags (Transponder)	MOBA-Artikel-Nummern 02-21-00000 bis 02-21-02000	
2	SW	Sicherheitskomponente der Fahrzeugsoftware MAWISMobilSecurity.dll	1.0.812.1	vom Hersteller installiert
3	SW	Sicherheitsmodul MawisSecurity.exe	1.0.808.1	vom Hersteller installiert oder als Installations-CD an den Auftraggeber
4	DOC	Handbuch Wartung MAWISMobil [9]	6	
5	DOC	Handbuch MAWIS Software MAWISMobil [10]	18	
6	DOC	Beschreibung der Anwendung MAWISSecurity.exe [11]	9	
7	DOC	Systemverwalterhandbuch [12]	10	

Tabelle 2: Auslieferungsumfang des EVG

Der EVG-Teil der Fahrzeugsoftware (MAWISMobilSecurity.dll) wird vom Hersteller als Teil der Fahrzeugsoftware installiert und zusammen mit dieser ausgeliefert. Die Versionsabfrage zum EVG-Teil der Fahrzeugsoftware ist im Handbuch MAWIS Software MAWISMobil [10] beschrieben.

Das Sicherheitsmodul wird ebenfalls vom Hersteller installiert. Die Versionsabfrage ist in der Beschreibung der Anwendung MAWISSecurity.exe [11] beschrieben.

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 Annahmen in den Sicherheitsvorgaben werden nicht durch den EVG selbst abgedeckt. Diese Aspekte setzen voraus, dass bestimmte Sicherheitsziele durch die EVG-Einsatzumgebung erfüllt werden. 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 3.1.

5 Informationen zur Architektur

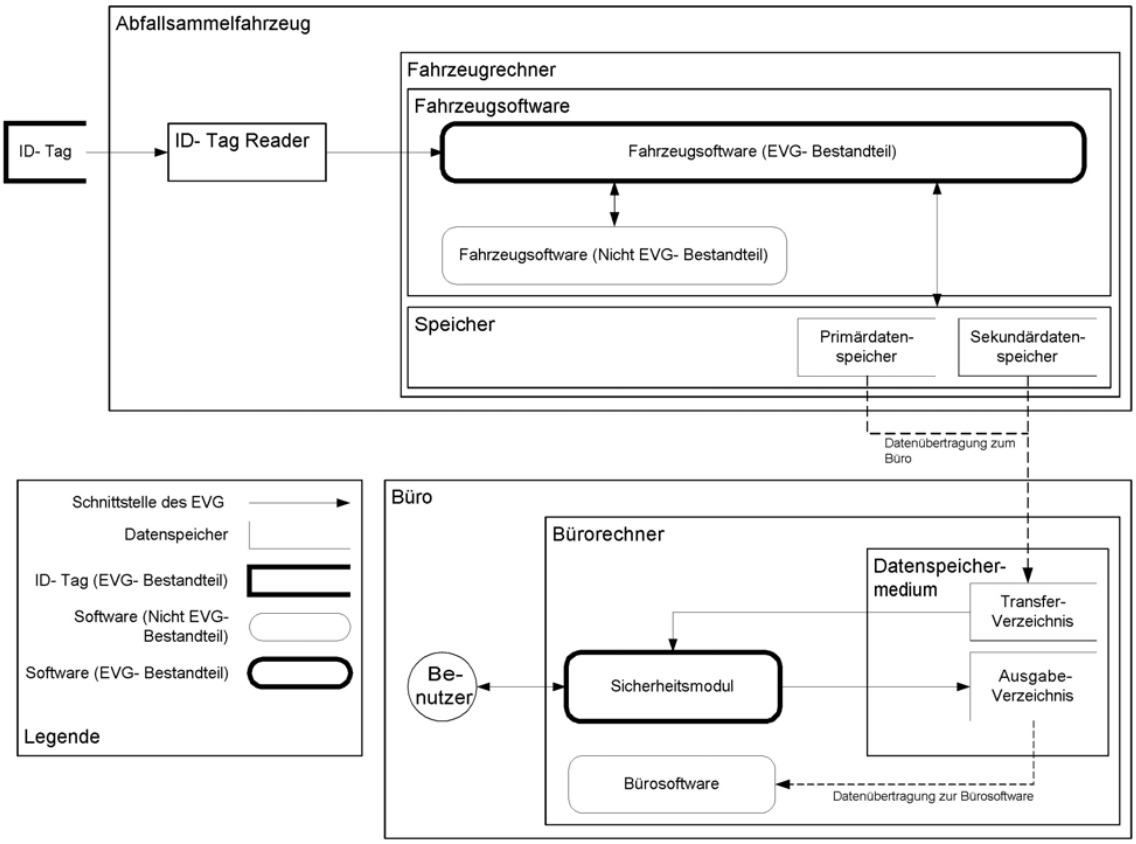

Abbildung 1: Überblick über das Abfallbehälter-Identifikationssystem

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 (Sicherheitskomponente MAWISMobilSecurity.dll) und dem nicht zum EVG gehörenden Teil der Fahrzeugsoftware. Im Fahrzeugrechner befindet dich außerdem der Sekundärdatenspeicher. Der Primärdatenspeicher ist ein externer Speicher, der in den Fahrzeugrechner eingelegt werden kann. Der Bürorechner beinhaltet neben der Bürosoftware das Sicherheitsmodul MawisSecurity.exe. Des Weiteren verfügt der Bürorechner über ein Datenspeichermedium zur Übertragung der Leerungsdaten. 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 vom Entwickler bereitgestellte Testkonfiguration bestand aus den Komponenten des EVG und des Produkts in der aktuellen Fassung. Der Entwickler hat alle des im Fahrzeug befindlichen Teile des Produktes zusammengestellt und die Teile miteinander verbunden.

Das Produkt war gemäß den Vorgaben im Handbuch bereits vorinstalliert. Die Installation der Software MawisSecurity.exe wurde vom Evaluator gemäß der Beschreibung im Handbuch nachvollzogen. Die Evaluatoren haben sich davon überzeugt, dass der in den Sicherheitsvorgaben [6] spezifizierte EVG für die Tests zur Verfügung stand.

Der Entwickler hat folgende Teile des Produktes zur Verfügung gestellt:

- Reader mit Antennen und Sensoren für Leergutposition: MOBA Ident-Control IDC20 Ser.-No. 2007 26 33; Firmware-Version IWA09530.hex
- MOBA Operand als Fahrzeugrechner: MOBA Operand Art.-No.: 04-55-01051, Ser.-No.: 2005268
- PC als Bürorechner: Laptop, AMD Athlon XP-M, XP Prof. 2002, Service Pack 2
- MOBA MemoryDrive (primärer Datenspeicher, gelb): Art.-No. 03-05-02040
- MOBA MemoryDrive (ServiceDrive, grün): Art.-No. 03-05-02041
- Auf Fahrzeugrechner: MAWISMobil.exe; Ver. 1.6.812.1
- EVG auf Fahrzeugrechner: MAWISMobilSecurity.dll; Ver. 1.0.812.1
- EVG auf Bürorechner: MawisSecurity.exe; Ver. 1.0.808.1
- Bürosoftware: RpfMawis Ver. 6.4.0.0

7.2 Zusammenfassung der unabhängigen Prüfstellentests

Es wurden alle Sicherheitsfunktionen des EVG an den zugänglichen Benutzerschnittstellen mit jeweils mindestens einem Testfall getestet, um das korrekte Verhalten der Sicherheitsfunktionen zu überprüfen.

Insgesamt zeigen die Tests, dass sich der EVG wie in den Sicherheitsvorgaben [6] spezifiziert verhält.

Für die postulierte Evaluationsstufe EAL 1 werden keine Herstellertests gefordert.

8 Evaluierte Konfiguration

Der EVG wird ausschließlich in einer Konfiguration betrieben. Er wird durch die Bezeichnung „Abfallbehälter-Identifikationssystem MAWIS Rev. 3.0 , bestehend aus der Sicherheitskomponente der Fahrzeugsoftware MAWISMobilSecurity.dll, Version 1.0.812.1 und dem Sicherheitsmodul MawisSecurity.exe, Version 1.0.808.1 sowie den Transpondern (ID-Tags) mit den MOBA-Artikel-Nummern 02-21-00000 bis 02-21-02000“ identifiziert.

Dieses Zertifikat bezieht sich ausschließlich auf diese Konfiguration des EVG.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen 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 Vertrauenswürdigkeitskomponenten bestätigt:

- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 1 der CC (siehe auch Teil C des Zertifizierungsreports)

Die Evaluierung hat gezeigt:

- PP Konformität — Protection Profile Waste Bin Identification System (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

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.

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 / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluierungsgegenstand (EVG)

IT Informationstechnologie

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

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SFP Security Function Policy – Politik der Sicherheitsfunktion

SOF Strength of Function – Stärke der Funktion

ST Security Target – Sicherheitsvorgaben

TOE Target of Evaluation –Evaluierungsgegenstand

TSC TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle

TSF	TOE Security Functions - EVG-Sicherheitsfunktionen
TSP	TOE security policy - EVG-Sicherheitspolitik
WBIS	Waste Bin Identification System – Abfallbehälter-Identifikationssystem

12.2 Glossary

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

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

Evaluationsgegenstand - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die TSP korrekt zu erfüllen.

EVG-Sicherheitspolitik - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

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

Informell - Ausgedrückt in natürlicher Sprache.

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

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Anwenderbedürfnisse erfüllen.

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

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlass sein muss.

Sicherheitsvorgaben - Eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

SOF-Hoch - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

SOF-Mittel - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Niedrig - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

Stärke der Funktionen - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

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

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

13 Literaturangaben

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

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

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

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

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

[6] Sicherheitsvorgaben BSI-DSZ-0496-2008, Version 34, 28.04.08, MAWIS, Rev. 3.0 Sicherheitsvorgaben für die Zertifizierung nach WBIS PP BSI-DSZ-CC-0496, MOBA Mobile Automation AG

[7] ETR: Evaluationsbericht BSI-DSZ-CC-0496 zu MAWIS, Rev. 3.0 der MOBA Mobile Automation AG, Version 3, 29.04.08, Tele-Consulting GmbH (vertrauliches Dokument)

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

[9] Handbuch Wartung MAWISMobil, Version 6, 04.03.08, MOBA Mobile Automation AG

[10] Handbuch MAWIS Software MAWISMobil, Version 18, 28.04.08, MOBA Mobile Automation AG

[11] Beschreibung der Anwendung MAWISSecurity.exe, Version 9, 28.04.08, MOBA Mobile Automation AG

[12] Systemverwalterhandbuch, Version 10, 28.04.08, MOBA Mobile Automation AG

C Auszüge aus den Kriterien

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

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Dies ist eine eingefügte Leerseite.