Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0496-V2-2025

zu

MAWIS-Security Rev. 4.0

der

MOBA Mobile Automation AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, 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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0496-V2-2025 (*)

Abfallbehälter-Identifikations-System

MAWIS-Security Rev. 4.0

von	MOBA Mobile Automation AG
PP-Konformität:	Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27 May 2004, 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, ASE_REQ.2
Gültig bis:	23. Januar 2030

SOGIS
Recognition Agreement

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 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 5 zu entnehmen.

Common Criteria
Recognition Arrangement

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, 24. Januar 2025

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Ingo Hahlen
Referatsleiter

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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.

Gliederung

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG1 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.

2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern und für Heimat
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

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

2 Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und - Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

3 Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt I S. 1365

4 Bekanntmachung des Bundesministeriums des Innern und für Heimat vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

3. 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.

3.1. Europäische Anerkennung von 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 (SOGIS Technical Domain) auf höheren Anerkennungsstufen fest.

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen EAL 1 bis EAL 4 ein. Für Produkte im technischen Bereich "smartcard and similar devices" ist eine SOGIS Technical Domain festgelegt. Für Produkte im technischen Bereich "HW Devices with Security Boxes" ist ebenfalls eine SOGIS Technical Domain festgelegt. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles) basierend auf den Common Criteria.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite https://www.sogis.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt mit allen ausgewählten Vertrauenswürdigkeitskomponenten unter die Anerkennung nach SOGIS-MRA.

3.2. Internationale Anerkennung von CC - Zertifikaten

Das internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA-2014) wurde am 8. September 2014 ratifiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis einschließlich EAL 2 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP).

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite https://www.commoncriteriaportal.org eingesehen werden.

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014 für alle ausgewählten Vertrauenswürdigkeitskomponenten.

4. 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-Security Rev. 4.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts MAWIS-Security Rev. 4.0 wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH durchgeführt. Die Evaluierung wurde am 13. Dezember 2024 abgeschlossen. Das Prüflabor Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

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.

5. Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes. Das Produkt ist 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 Vertrauenswürdigkeitskomponenten und -stufen kann direkt den CC entnommen werden. Detaillierte Referenzen sind in Teil C dieses Reportes aufgelistet.

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 Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 24. Januar 2025, ist gültig bis 23. Januar 2030. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

[5] Information Technology Security Evaluation Facility

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
3. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, bei denen die Zertifizierung des Produktes aber von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.

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. Veröffentlichung

Das Produkt MAWIS-Security Rev. 4.0 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[6]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[6] MOBA Mobile Automation AG
Kapellenstraße 15
65555 Limburg
Deutschland

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 EVG, MAWIS-Security Rev. 4.0 ist ein Abfallbehälteridentifikationssystem, bestehend aus dem Sicherheitsmodul der Fahrzeugsoftware MAWIS-MobilSecurity, dem Sicherheitsmodul der Bürosoftware MAWIS-OfficeSecurity, sowie den Transpondern (ID-Tags) und Handbüchern. Er wird im Bereich der Abfallentsorgung eingesetzt, wo Abrechnungssysteme gefordert werden, die eine verursacherbezogene Gebührenabrechnung über die Anzahl der Leerungen ermöglichen.

Die an Abfallbehälter montierten ID-Tags enthalten eindeutige Identifikationsdaten eines Abfallbehälters. Während des Leerungsvorganges der Abfallbehälter durch das Abfallsammelfahrzeug werden deren ID-Tags ausgelesen und identifiziert.
Die Identifikationsdaten werden auf dem Fahrzeug durch weitere Informationen ergänzt und für die Gebührenabrechnung an die Bürosoftware gesendet.

Der EVG bietet Schutz vor Datenverlust und rein zufälliger Datenverfälschung während der Speicherung im ID-Tag und im Abfallsammelfahrzeug, sowie während der Übertragung vom ID-Tag zur Fahrzeugsoftware (MAWIS-MobileSecurity) und von der Fahrzeugsoftware zur Bürosoftware (MAWIS-OfficeSecurity).

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

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [9].

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, 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 folgende Sicherheitsfunktionalität des EVG umgesetzt:

Sicherheitsfunktionalität des EVG	**Thema**
TSF_TagID_Check	Integritätsprüfung von Transponder-Ids im Sicherheitsmodul der Fahrzeugsoftware
TSF_GenerateAT_Check	Generierung von Leerungsdatensätzen sowie Gültigkeits- und Integritätssicherung im Sicherheitsmodul der Fahrzeugsoftware
TSF_GenerateATPlus_Check	Generierung von Leerungsdatenblöcken sowie Gültigkeits- und Integritätssicherung im Sicherheitsmodul der Fahrzeugsoftware
TSF_Store_ATPlus	Redundante Speicherung von Leerungsdatenblöcken auf dem Fahrzeugrechner
TSF_Check_ATPlus	Gültigkeits- und Integritätsprüfung der Leerungsdatenblöcke im Sicherheitsmodul der Bürosoftware

Sicherheitsfunktionalität des EVG	Thema
TSF_Check_AT	Gültigkeits- und Integritätsprüfung der Leerungsdatensätze im Sicherheitsmodul der Bürosoftware

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 7.1 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 3.1 – 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-Security Rev. 4.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Bezeichnung	Version	Auslieferungsart
1	HW	ID-Tags	Texas Instruments: TRPGR30ENATGA TRPGR30ENATGB EM Microelectronic: EM4205 EM4305 Silicon Craft: SIC279 Impinj: Impinj Monza 4QT NXP: UCODE G2iM+	Die Transponder werden durch den Hersteller an den Kunden ausgeliefert.

Nr	Typ	Bezeichnung	Version	Auslieferungsart
2	SW	MAWIS-MobilSecurity[7] (EVG-Teil der Fahrzeugsoftware)	Modulname/-format bei MOBA Operand und kompatible: Mawis.MobileSecurity.dll, Version 4.1.2310.7 Modulname/-format bei MOBA Mini Operand und kompa-tiblen Android-Geräten: De.Moba.Mawis.MobileSecurity.dll, Version 4.1.2318.10 Modulname/-format bei MOBA CG1 und kompatible: MAWISsecurity.lib, Version 4.1.2234.0	Wird dem Endbenutzer bei Übergabe des MAWIS-Systems vorinstalliert auf der jeweiligen Hardware bereitgestellt.
3	SW	MAWIS-OfficeSecurity (EVG-Teil der Bürosoftware)	Modulname/-format: De.Moba.Mawis.OfficeSecurity.dll, Version 4.1.2318.11	Wird dem Endbenutzer bei Übergabe des MAWIS-Systems vorinstalliert auf der jeweiligen Hardware bereitgestellt.
4	DOC	MAWIS-Security, Rev 4.0 Betriebsanleitung	Art-No.: 10-02-00416, Version 5.0	Die Bereitstellung erfolgt als PDF-Datei auf einem elektronischen Datenträger oder per Mail.
5	HW/ SW	Fahrzeugrechner (Nicht-EVG)	Hardware-Anforderungen: ● MOBA Operand oder MOBA Mini Operand oder CG1 oder kompatible ● CWG-200 (nur bei Verwendung des CG1 als Fahrzeugrechner) Software/Firmware-Anforderungen: ● Auf MOBA Operand oder kompatible: MAWISMobil.exe, Version 3.15.1926.42[8] ● Auf MOBA Mini Operand oder kompatible: MAWISapp, Version 4.0.2327.0[8] (enthalten in de.moba.mawisapp.apk) ● Auf CG1 oder kompatible: MAWIScompact, Version 4.2.2322.0[8] ● Auf CWG-200: CWG BS512 Version 1.1.2229.0[8]	Wird dem Endbenutzer bei Übergabe des MAWIS-Systems vorinstalliert auf der jeweiligen Hardware bereitgestellt.
6	SW	Serverseitiger Teil der Bürosoftware (Nicht-EVG)	Datahandler: EmptyingServiceDataHandler.dll, Version 2.41.2320.3[8] MAWIS-OfficeSecurity Adapter: MawisOfficeSecurity.Adapter.dll, Version 2.41.2320.3[8]	Wird dem Endbenutzer bei Übergabe des MAWIS-Systems vorinstalliert auf der jeweiligen Hardware bereitgestellt.

Tabelle 2: Auslieferungsumfang des EVG

[7]Gleichbedeutende alternative Schreibweise: MAWIS-MobileSecurity

[8]Die genannten Software-Komponenten dürfen für Fehlerkorrekturen oder kundenspezifische Anpassungen geringfügig geändert werden. Der Aufruf des EVG darf dadurch nicht verändert werden. Fehlerkorrekturen spiegeln sich im letzten Teil der Versionsnummer wider.

3. Sicherheitspolitik

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

- Integritätsschutz von Identifikationsdaten, Leerungsdatensätzen und Leertungsdatenblöcken bei der Speicherung im Fahrzeug und bei der Übertragung zwischen materiell getrennten Teilen des EVG
- Gültigkeitsnachweis von Leerungsdatensätzen und Leerungsdatenblöcken
- Schutz vor Verlust von Leerungsdatensätzen durch redundante Speicherung im Fahrzeug

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 die folgenden Punkte relevant:
An den Abfallbehältern fest verbaute Transponder mit eindeutigen IDs, vertrauenswürdiges Personal, wirksamer Zugangsschutz zu SW-Bestandteilen des EVG, Überprüfung der Vollständigkeit der übertragenen Daten und Datensicherung in der Büro-Einsatzumgebung.
Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5. Informationen zur Architektur

Der EVG besteht aus drei materiell vollständig voneinander getrennten Teilsystemen:

- Kommerziell gebrauchsfertige ID-Tags (RFID-Transponder)
- Sicherheitsmodul MOBA-MobilSecurity (Bestandteil der Fahrzeugsoftware)
- Sicherheitsmodul MOBA-OfficeSecurity (Bestandteil der Bürosoftware)

Die Interaktion zwischen den Teilsystemen wird von der IT-Umgebung durchgeführt und erfolgt durch Übertragung

- vom ID-Tag zum Sicherheitsmodul MOBA-MobilSecurity (Identifikationsdaten mit CRC-Prüfwert) und
- vom Sicherheitsmodul MOBA-MobilSecurity zum Sicherheitsmodul MOBA-OfficeSecurity (Leerungsdatenblöcke mit Fahrzeugkennung als Gültigkeitsmerkmal und mit CRC-Prüfwerten für Leerungsdatenblöcke und darin enthaltene Leerungsdatensätze)

Die Verarbeitung von Leerungsdatensätzen und -blöcken wird durch redundante Speicherung im Fahrzeugrechner von der Übertragung zum Bürorechner entkoppelt.

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

Für die unabhängigen Funktionstests hat der Hersteller die drei Fahrzeugrechner voll funktionsfähig in Form eines Demonstrators zur Verfügung gestellt. Die jeweilige Testumgebung enthielt eine Auswahl der RFID-Transponder, die Fahrzeugrechner mit den dazugehörigen Antennen, RFID-Empfängern, Speichereinheiten und Sendemodulen für die Mobilfunkanbindung an den Server. Die Versionen der EVG-Module und der Firmware, in die sie eingebettet waren stimmten mit den im ST und der Konfigurationsliste aufgeführten Versionen überein. Vor jedem Test wurde auf Fehlermeldungen geachtet und somit sichergestellt, dass der EVG in einem fehlerfreien Zustand betrieben wurde.

Die Fahrzeugrechner wurden vom Hersteller voll konfiguriert an das Prüflabor ausgeliefert. Der Server stand während der beiden Testtage ausschließlich für die Tests zur Verfügung. Dort waren Fahrzeugkennungen der drei Fahrzeugrechner im Test und der Zugang für diese über Mobilfunk eingerichtet. Die Verbindung zu den Servern konnte entsprechend der Anzeige der Fahrzeugrechner erfolgreich aufgebaut werden. Zu Beginn der Tests wurde generell auf von den Fahrzeugrechnern gemeldete Fehler geachtet. Diese sind nur dann aufgetreten, wenn diese wegen der für den Test vorgenommenen Vorkehrungen zu erwarten waren. Die Umgebung der EVG-Komponente auf dem Server war so konfiguriert, dass sie mit den drei Fahrzeugrechnern korrekt zusammenarbeitet.

Die evaluierten Konfigurationen wurden vollständig getestet.

7.2. Zusammenfassung der unabhängigen Prüfstellentests

Für alle Sicherheitsfunktionen und funktionalen Sicherheitsanforderungen wurden Positiv- und Negativ-Tests entwickelt und durchgeführt. Dabei wurden alle Schnittstellen der funktionalen Spezifikation abgedeckt. Die Stimulation dieser Schnittstellen und Beobachtung der Aktionen erfolgte grundsätzlich über geeignete Eingaben und Ausgaben an den mit den externen Schnittstellen der Fahrzeug- und Bürosoftware verbundenen Komponenten. In allen Fällen entsprachen die tatsächlichen Testergebnisse den erwarteten Testergebnissen.

Im Rahmen der Schwachstellenanalyse wurden für das angenommene Angriffspotential (AVA_VAN.1 – basic attack potential) keine Schwachstellen gefunden.

8. Evaluierte Konfiguration

Der EVG kann in drei verschiedenen Konfigurationen betrieben werden. Die Konfigurationen unterscheiden sich durch die verwendeten Fahrzeugrechner (MOBA Operand, MOBA Mini Operand, CG1 - nicht-EVG) und die dafür vorgesehene Fahrzeugsoftware. Die drei Konfigurationen (auch in Kombination) entsprechen dem Gegenstand der Evaluierung, beinhalten die Komponenten zur Ansteuerung der EVG-Komponenten in der Fahrzeug- und Bürosoftware und können mit allen identifizierten ID-Tags (RFID-Transponder) betrieben werden.
Die zu den evaluierten Konfigurationen gehörigen Versionen der EVG-Bestandteile und der ansteuernden Komponenten sind in Tabelle 2 aufgeführt.

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 verwendet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeitskomponenten bestätigt:

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

Die Evaluierung hat gezeigt:

- PP Konformität: Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27 May 2004, BSI-PP-0010-2004 [8]
- 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, 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 kryptographischen Mechanismen. Folglich waren solche Mechnismen nicht Gegenstand der Evaluierung.

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.

Über die Betriebsdokumentation hinaus ist folgendes bei der Nutzung des EVG in seinen evaluierten Konfigurationen zu beachten:

- Das Sicherheitsmodul MOBA-MobilSecurity verarbeitet auch Identifikationsdaten von ID-Tags (RFID Transponder), die nicht zur evaluierten Konfiguration des EVG gehören. Um die Erkennung von Manipulationen der Identifikationsdaten zu gewährleisten, müssen solche Fälle vermieden werden.

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.

Zertifizierte Aktualisierungen des EVG, die die Vertrauenswürdigkeit betreffen, sollten verwendet werden, sofern sie zur Verfügung stehen. Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte der Anwender den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen. In der Zwischenzeit sollte der Risikomanagementprozess für das IT-System, in dem der EVG eingesetzt wird, prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müssen, um die Systemsicherheit aufrecht zu erhalten.

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 / Act on the Federal Office for Information Security

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

CRC Cyclic Redundancy Code

cPP Collaborative Protection Profile

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluierungsgegenstand

ETR Evaluation Technical Report

IT Information Technology - Informationstechnologie

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

PP Protection Profile - Schutzprofil

SAR Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen

SF Security Function - Sicherheitsfunktion

SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
ST	Security Target - Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
WBIS	Waste Bin Identification System - Abfallbehälter-Identifikationssystem

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.

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 implementierungsabhängige Menge von Sicherheitsanforderungen 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
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI-Zertifizierung: Verfahrendokumentation zum Zertifizierungsprozess (CC-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[9] https://www.bsi.bund.de/AIS

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/zertifizierungsreporte

[6] Sicherheitsvorgaben BSI-DSZ-0496-V2-2025, MAWIS-Security, Rev. 4.0 Sicherheitsvorgaben nach WBIS-PP, Version 4.3, 23.10.2024, MOBA Mobile Automation AG

[7] Evaluation Technical Report - Evaluierung MAWIS-Security 4.0, Version 1.0, 13.12.2024, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH (vertrauliches Dokument)

[8] Protection Profile – Waste Bin Identification Systems (WBIS-PP), BSI-PP-0010-2004, Version 1.04, Deutscher Städte- und Gemeindebund und Bundesamt für Sicherheit in der Informationstechnik

[9] MAWIS-Security, Rev. 4.0 – Konfigurationsliste zur Zertifizierung nach CC und WBIS-PP, Version 4.3, 23.10.2024, MOBA Mobile Automation AG

[10] MAWIS-Security, Rev 4.0 Betriebsanleitung, Version 5.0, 23.04.2024, MOBA Mobile Automation AG

[9] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC können dazu genutzt werden:

- Definition und Beschreibung zu Conformance Claims: CC Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -kompomenten: CC Teil 3 Kapitel 7.1
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 3 Kapitel 7.2 und 8
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC Teil 3 Kapitel 12
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC Teil 3 Kapitel 13 bis 17
- Die Tabelle in CC Teil 3 Anhang E fasst die Beziehung zwischen den Vertrauenswürdigkeitsstufen (EAL) und den Vertrauenswürdigkeitsklassen, -familien und -komponenten zusammen.

Die Common Criteria sind unter https://www.commoncriteriaportal.org/cc/ veröffentlicht.

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Bemerkung: Ende des Reportes