MAWIS-Security, Rev. 4.0

Sicherheitsvorgaben nach WBIS-PP

Dokumentversion 4.3

Inhaltsverzeichnis

Glossar

Tabelle 1 Begriffserklärungen

Begriff / Abkürzung	Erklärung
Identification Unit bzw. Identifikationseinheit	ID-Tag oder Transponder, der die Identifikationsdaten eines Abfallbehälters trägt. Er ist am Abfallbehälter (meist unter dem oberen Rand) befestigt und wird während des Entleerungsprozesses vom Reader ausgelesen.
MAWIS	**M**OBA **A**utomatic **W**aste **I**dentification **S**ystem Produktbezeichnung für das Abfall-Behälter-Identifikations-system von MOBA.
ID-Tag	Siehe Identification Unit
Transponder	Siehe Identification Unit
Transponder-ID	In einem Transponder gespeicherte Identifikationsdaten. Sie können durch einen Reader ausgelesen werden.
Ident-Control (IDC)	Bezeichnung des Readers der Firma MOBA Mobile Automation AG
MOBA Operand	Bezeichnung eines Fahrzeugrechners der Firma MOBA Mobile Automation AG
CG1	Bezeichnung eines Fahrzeugrechners der Firma MOBA Mobile Automation AG
MOBA Mini Operand	Bezeichnung eines Fahrzeugrechners der Firma MOBA Mobile Automation AG
CRC	Cyclic Redundancy Check Die zyklische Redundanzprüfung (englisch *cyclic redundancy check*, daher meist CRC) ist ein Verfahren zur Bestimmung eines Prüfwerts für Daten, um Fehler bei der Übertragung oder Speicherung erkennen zu können. Synonym für den Prüfwert wird auch häufig der Begriff *Checksumme* verwendet.
CRC32	ist ein 32-Bit-CRC-Wert

1 ST- Einführung

Dieses Security Target beschreibt die Vorgaben für das Behälteridentifikationssystem MAWIS für die Zertifizierung des Produktes nach Common Criteria for Information Technology Security Evaluation ([1], [2], [3]) sowie nach dem Schutzprofil WBIS-PP [4].

Das Security Target enthält Passagen, die aus dem WBIS-PP [4] übernommen wurden. Diese Passagen sind in blauer Schrift gehalten. Alle anderen Texte sind mit schwarzer Schrift verfasst.

1.1 ST- Identifikation

Titel: MAWIS-Security, Rev. 4.0 - Sicherheitsvorgaben nach WBIS-PP
Autor: Stephan Holz, MOBA Mobile Automation AG

ST- Version: 4.3
ST- Datum: 23.10.2024

1.2 EVG- Identifikation

Name: MAWIS-Security
Version: 4.0

1.3 EVG- Übersicht

Ziel dieser Sicherheitsvorgaben ist es, die funktionalen Anforderungen und Vertrauenswürdigkeitsanforderungen für die EVG-Teile *MAWIS-Security* des Abfallbehälter-Identifikationssystems (WBIS[1]) MAWIS zu spezifizieren.

Die Sicherheitsvorgaben definieren die Sicherheitsanforderungen dieser EVG-Teile für die Übertragung und Speicherung der aufgezeichneten Leerungsdaten.

Der EVG *MAWIS-Security* ist vom Gesamtsystem MAWIS abgegrenzt. MAWIS und *MAWIS-Security* setzen keine zusätzlichen Funktionen und Sicherheitsanforderungen um.

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

Aufgabe von Systemen dieser Art ist es zu zählen, wie oft die Behälter geleert worden sind, um auf diese Art eine verursacherbezogene Abrechnung der Abfallgebühren zu ermöglichen.

MAWIS ist ein solches Abfall-Behälter-Identifikationssystem (WBIS), das im Rahmen der regelmäßigen Mülltonnenleerung den Entleerungsvorgang von Abfallbehältern erfasst. Dazu ist jeder Abfallbehälter mit einem RFID-Chip (ID-Tag) versehen. Dessen Identifikationsnummer (ID) wird beim

[1] WBIS – **W**aste **B**in **I**dentificaton **S**ystem: Abfallbehälter-Identifikationssystem

Entleeren der Mülltonne automatisch erfasst, gespeichert und für die Gebührenabrechnung zur Verfügung gestellt. Durch die eindeutige Zuordnung der ID zum Verursacher ermöglicht dies eine auf Menge und Verursacher ausgerichtete Abrechnung von Müllgebühren.

Häufig werden solche Systeme auch mit zum Beispiel einem Wiege- oder einem Volumenmesssystem kombiniert, um die Entsorgungsleistungen nach Häufigkeit und nach Gewicht oder Menge abrechnen zu können. Es sind in Zukunft auch andere Verfahren denkbar und mit dem System einsetzbar, die dem Entsorger zusätzliche für ihn notwendige Informationen verschaffen. Dazu gehören zum Beispiel Informationen über Wartungszyklen oder über Besonderheiten, die während der Bearbeitung des Entleerungsauftrages aufgetreten sind. Solche optionalen Systeme und andere ergänzende Verfahren gehören jedoch nicht zum EVG.

Abfall-Behälter-Identifikationssysteme (WBIS) basieren auf der elektronischen Erfassung, Übertragung und Speicherung von Leerungsdaten (als Leistungsnachweise von den Entsorgungsunternehmen) bis hin zur Erstellung eines Abfall-Gebührenbescheides durch die entsorgungspflichtigen Körperschaften (Städte und Landkreise) bzw. Rechnungsstellung durch den Entsorger. Weil aufgrund der Masse der anfallenden Daten eine manuelle Detailprüfung jeder abgerechneten Leerung ausgeschlossen ist, benötigen solche Systeme ein hohes Maß an Vertrauen in die technische Funktionsfähigkeit des Systems, dass nur genau die tatsächlich durchgeführten Leerungen abgerechnet und dem richtigen Verursacher (hier Abfallbehälter) zugeordnet werden.

Um dem Wunsch nach Vertrauen Rechnung zu tragen, wurden MAWIS mit Sicherheitskomponenten ausgestattet. Die MAWIS-Sicherheitskomponenten sind unter dem Begriff *MAWIS-Security* zusammengefasst. Somit sind durch MOBAs Abfall-Behälter-Identifikationssystem MAWIS die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vor Manipulation und Verlust geschützt. Geschützt werden auch zusätzlich optional während des Leerungsprozesses erfasste Daten. Der Manipulationsschutz zielt hierbei auf den Schutz gegen zufällige Verfälschungen.

1.3.1 Verwendung und wichtige Sicherheitsmerkmale von MAWIS-Security

Die an Abfallbehälter montierten ID-Tags (EVG-Teil) enthalten eindeutige Identifikationsdaten eines Abfallbehälters. Während des Leerungsvorganges der Behälter durch das Abfallsammelfahrzeug werden deren ID-Tags identifiziert.

Durch das Sicherheitsmodul *MAWIS-MobilSecurity* wird die Integrität der Identifikationsdaten überprüft. Ausgehend von der Identifizierungsnummer des Behälters bildet *MAWIS-MobilSecurity* einen Leerungsdatensatz und ergänzt ihn um einen Zeitstempel sowie zusätzliche Leerungsinformationen. Der Leerungsdatensatz wird mit einem Integritätsmerkmal versehen. In die Bildung des Integritätsmerkmals wird zusätzlich die Fahrzeugkennung als Gültigkeitsmerkmal einbezogen.

Im Verlauf oder nach Abschluss einer Leerungstour des Fahrzeuges werden alle gesammelten Daten durch die Fahrzeugsoftware drahtlos an einen Server übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Dazu fasst *MAWIS-MobilSecurity* die Leerungsdatensätze zu einem Leerungsdatenblock zusammen, versieht ihn mit einem Gültigkeits- sowie einem Integritätsmerkmal und speichert ihn redundant im Fahrzeugrechner. Durch den nicht zum EVG gehörenden Teil der Fahrzeugsoftware wird der Leerungsdatenblock an den Bürorechner (Server) übertragen.

Dort werden die empfangenen Leerungsdatenblöcke zum Sicherheitsmodul *MAWIS-OfficeSecurity* übertragen. Das Sicherheitsmodul prüft Integrität und Gültigkeit jedes Leerungsdatenblockes und

jedes enthaltenen Leerungsdatensatzes, erzeugt eine Information über das Prüfergebnis und speichert Leerungsdatenblöcke, -sätze und Prüfergebnis in einem zentralen Datenbestand der Bürosoftware.

Von hier aus können diese Daten regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet oder direkt von Abrechnungssoftware verwendet werden.

1.3.2 Erforderliche Nicht- EVG Hardware/Software/Firmware

Tabelle 2 Fahrzeugseitig

Komponente	Anforderungen
Reader	Kompatibel entsprechend DIN 30745 Interface zum Fahrzeugrechner (z.B. CAN)
Fahrzeugrechner	Hardware-Anforderungen • MOBA Operand oder MOBA Mini Operand oder CG1 oder kompatible • CWG-200 (nur bei Verwendung des CG1 als Fahrzeugrechner) • Internetanbindung • Interface zur Kommunikation mit den restlichen fahrzeugseitigen Komponenten (z.B. CAN, Bluetooth, WLAN) Software/Firmware-Anforderungen • Auf MOBA Operand oder kompatible: MAWISMobil.exe, Version 3.15.1926.42* • Auf MOBA Mini Operand oder kompatible: MAWISapp, Version 4.0.2327.0 * (enthalten in de.moba.mawisapp.apk) • Auf CG1 oder kompatible: MAWIScompact, Version 4.2.2322.0 * • Auf CWG-200: CWG BS512 Version 1.1.2229.0 * 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 (siehe auch Abschnitt „Information zur Versionierung“).

Tabelle 3 Serverseitig

Komponente	Anforderungen
Server- und Betriebssystem-umgebung	Hardware-Anforderungen • CPU mindestens 2GHz, Kerne 2 • Speicher: RAM > 16GB, HDD/SSD >500GB • Mindestens durch Firewall geschützte Internetanbindung Software/Firmware-Anforderungen • Betriebssystem ab Windows Server 2012 • Datenbanksystem MSSQL Server ab 2012 • IIS, ab 8.0, Erreichbarkeit aus dem Internet • .NET ab Version 4.6.1 • MIP (MOBA-Internet-Plattform) ab Version 2.40
Serverseitiger Teil der Bürosoftware	• Datahandler: EmptyingServiceDataHandler.dll,Version 2.41.2320.3 *

* Erläuterung siehe Abschnitt *Information zur Versionierung* auf Seite 15

Komponente	Anforderungen
	• MAWIS-OfficeSecurity Adapter: MawisOfficeSecurity.Adapter.dll, Version 2.41.2320.3 * 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 (siehe auch Abschnitt „Information zur Versionierung“).

1.4 EVG-Beschreibung

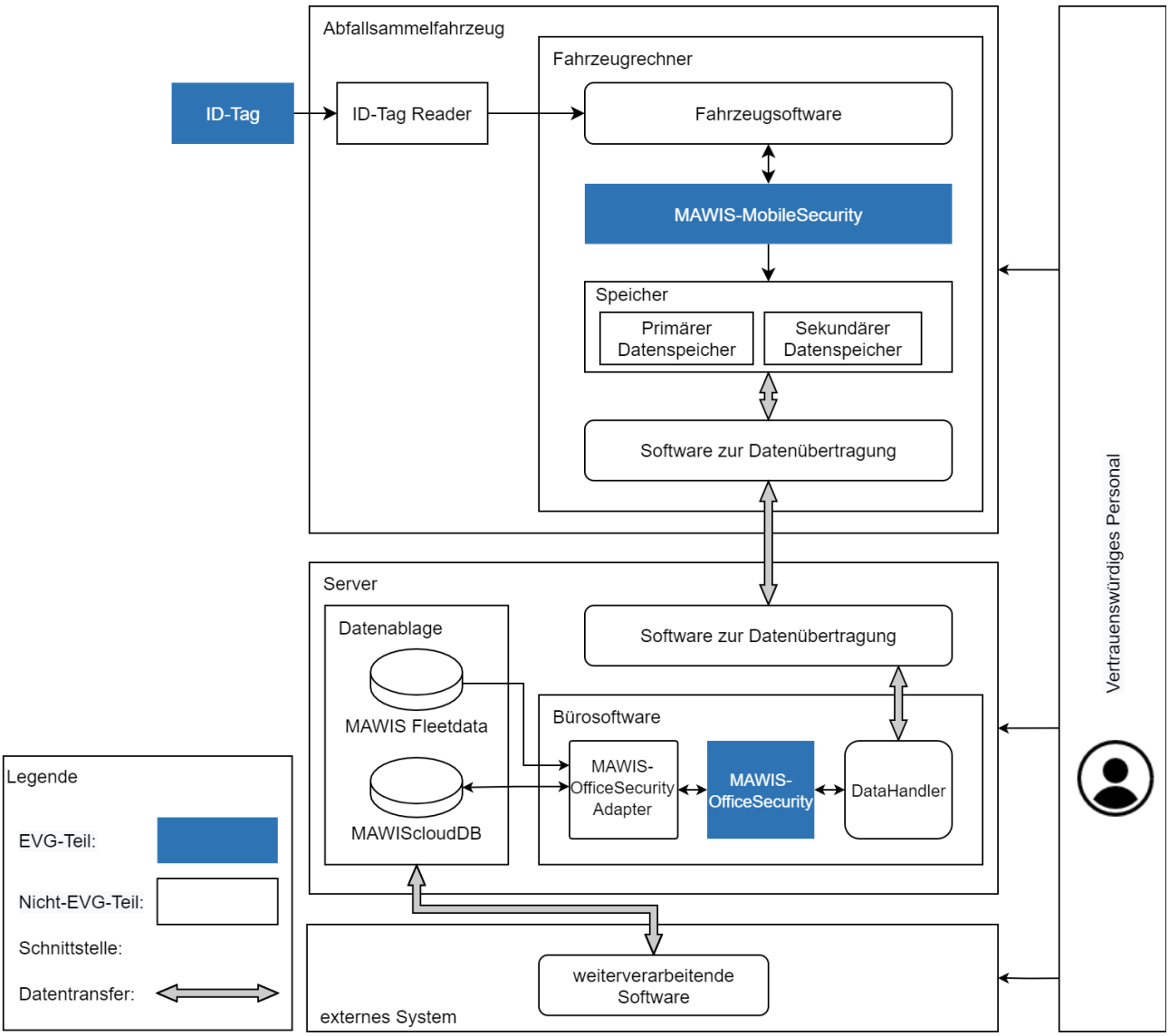
1.4.1 Allgemeiner Überblick über den EVG und dessen Sicherheitsfunktionen

Das Abfall-Behälter-Identifikationssystem MAWIS besteht aus folgenden Komponenten. Die Teile des EVG *MAWIS-Security* (ID-Tag, Sicherheitsmodule MAWIS-MobilSecurity und MAWIS-OfficeSecurity) sind hervorgehoben dargestellt (fett und kursiv):

- ***ID-Tag*** mit den Identifizierungsdaten des Abfallbehälters
- Abfallsammelfahrzeug mit dem (ID-Tag-) Reader, Fahrzeugrechner und einem optionalen Wiege-, Volumenmess- oder ähnlichem System. Die Fahrzeugsoftware mit dem fahrzeugseitigen ***Sicherheitsmodul MAWIS-MobilSecurity*** ist auf dem Fahrzeugrechner installiert.
- Bürorechner im Büro. Das büroseitige ***Sicherheitsmodul MAWIS-OfficeSecurity*** und die Bürosoftware sind installiert auf einem Server.

Abbildung 1 gibt einen Überblick über das Abfall-Behälter-Identifikationssystem (WBIS) MAWIS sowie dessen EVG-Teile.

Abbildung 1 *Überblick MAWIS- Komponenten und EVG-Teile*



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

Das System bietet die Möglichkeit, die Abrechnung über die Anzahl der Leerungen eines Abfallbehälters durchzuführen. Das System kann optional z.B. ein Wiege- oder Volumenmesssystem enthalten, um auch zur gewichtsbezogenen Abrechnung benutzt zu werden. Andere ergänzende Verfahren sind in der Zukunft möglich. Solche optionalen Systeme und andere ergänzende Verfahren gehören jedoch nicht zum EVG.

Die für die Abrechnung zugrunde gelegten Leerungsdaten entstehen bei der Leerung eines Abfallbehälters an einem Sammelfahrzeug, indem ausgehend von der Identifizierungsnummer des Behälters ein Leerungsdatensatz gebildet wird.

Die Abfallbehälter werden mit einem Datenträger (***ID-Tag***) ausgestattet. Der ***ID-Tag*** speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Es kommen ausschließlich Transponder zum Einsatz, deren Identifizierungsdaten beim Hersteller programmiert werden und danach nicht wieder modifiziert werden können (Read Only- Transponder). Darüber hinaus enthalten die zum Einsatz kommenden Transponder einen CRC- Prüfwert, der über dessen Daten gebildet und durch den ID-Tag mit den Identifizierungsdaten versendet wird. Diese Daten sind eindeutig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während der Leerung eines Abfallbehälters durch den Reader ausgelesen. Die Identifizierungsdaten werden dann an die Fahrzeugsoftware im Fahrzeugrechner weitergeleitet. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden erkannt. 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 die Identifizierungsdaten um Datum- und Zeitangaben und bildet daraus einen Leerungsdatensatz. Jeder erzeugte Leerungsdatensatz wird gegen Manipulation geschützt und redundant gespeichert. Zum Leerungsdatensatz können optional die Erfassungsdaten der zusätzlichen optionalen Komponenten abgespeichert werden. Solche optionalen Erfassungseinrichtungen gehören jedoch nicht zum EVG.

Im Verlauf oder nach Abschluss einer Leerungstour werden die gesammelten Leerungsdatensätze zu einem Leerungsdatenblock zusammengefasst. Der Leerungsdatenblock wird mit einem Gültigkeitsmerkmal versehen und gegen Manipulation geschützt. Er wird anschließend redundant gespeichert und zur Übertragung zum Bürorechner bereitgestellt. Optional kann der Datenblock zusätzliche Informationen enthalten. Dazu gehören beispielsweise die während der Entleerungen von einer Waage ermittelten Abfallgewichte. Der Leerungsdatenblock wird vom Abfallsammelfahrzeug zum Server übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Die Übertragung erfolgt drahtlos. Übertragungsstrecke und –verfahren gehören nicht zum EVG. Die optionalen Informationen werden ebenfalls nicht vom EVG betrachtet.

Die Leerungsdatenblöcke werden über das Sicherheitsmodul an die Bürosoftware übermittelt. Die Fahrzeugsoftware sorgt durch geeignete Maßnahmen dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist. Wird durch das Sicherheitsmodul im Bürorechner die Ungültigkeit übergebener Leerungsdatenblöcke festgestellt, können diese wiederholt aus einem sekundären Datenspeicher im Fahrzeugrechner zum Bürorechner übertragen werden. Leerungsdatenblöcke werden mindestens 2 Monate[2] im sekundären Datenspeicher vorgehalten und können innerhalb dieses Zeitraumes wiederholt übertragen werden.

Bei der Übermittlung der Leerungsdatenblöcke an die Bürosoftware wird durch das Sicherheitsmodul ***MAWIS-OfficeSecurity*** sichergestellt, dass nur die in einem Fahrzeug erstellten Datenblöcke als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt, indem übertragene Leerungsdatenblöcke durch das Sicherheitsmodul im Bürorechner auf Vollständigkeit, Integrität und Authentizität untersucht werden. Gültige und integre Leerungsdatensätze und Leerungsdatenblöcke werden weiterverarbeitenden Systemen in einer Datenbank als MAWIS Events zur Verfügung gestellt und können regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

[2] gilt für unterstellte tägliche Leerung von 3000 Behältern an einem Fahrzeug

Der ***ID-Tag*** und die Datenübertragungsstrecke zwischen dem ID-Tag und der Fahrzeugsoftware, die im Fahrzeug gespeicherten Daten sowie die Übertragungstrecke zwischen der Fahrzeugsoftware und dem Sicherheitsmodul sind potenziellen Angriffen ausgesetzt. Bei der Betrachtung des Angriffspotenzials muss der potenzielle Wert der zu schützenden Daten in Betracht gezogen werden. Dieser Wert ist als gering zu sehen. Es wird deshalb ein niedriges Angriffspotential angenommen. Der Zugang zu der Fahrzeugsoftware und zum Sicherheitsmodul ist durch geeignete physikalische und organisatorische Maßnahmen nur autorisiertem Personal möglich. Dieser Schutz wird durch das Fahrzeug mit seinen Komponenten und durch das Büro mit dem Bürorechner realisiert.

1.4.2 Abgrenzung des EVG

1.4.2.1 Physische Abgrenzung des EVG

Tabelle 4 listet die ausgelieferten Komponenten des EVG.

Tabelle 4 Liste der auszuliefernden Komponenten von MAWIS-Security

Komponente	Typ / Kurzbeschreibung	Version oder Referenz
ID-Tag	Hardware / ID-Tags sind passive Transponder, die eine eindeutige ID sowie einen Prüfwert (CRC) enthalten. Die ID-Tags werden an Abfallbehältern befestigt. Die auf den ID-Tags gespeicherten Informationen können von einem Lesegerät gelesen werden und dienen der Identifikation des Abfallbehälters.	Siehe Anhang 1
MAWIS-MobilSecurity	Software / *MAWIS-MobilSecurity* ist ein Sicherheitsmodul in Form einer Software-Bibliothek. Es ist der EVG-Teil der Fahrzeugsoftware. Modulname/-format bei MOBA Operand und kompatible: Mawis.MobileSecurity.dll Modulname/-format bei MOBA Mini Operand und kompatiblen Android-Geräten: De.Moba.Mawis.MobileSecurity.dll Modulname/-format bei MOBA CG1 und kompatible: MAWISsecurity.lib Die Fahrzeugsoftware verwendet das Sicherheitsmodul *MAWIS-MobilSecurity*, sie ist aber selbst nicht Bestandteil des EVG.	4.1.2310.7 * 4.1.2318.10 * 4.1.2234.0 *
MAWIS-OfficeSecurity	Software / *MAWIS-OfficeSecurity* ist ein Sicherheitsmodul in Form einer Software-Bibliothek. Es ist der EVG-Teil der Bürosoftware. Modulname/-format: De.Moba.Mawis.OfficeSecurity.dll Die Bürosoftware verwendet das Sicherheitsmodul *MAWIS-OfficeSecurity*, sie ist aber selbst nicht Bestandteil des EVG.	4.1.2318.11 *
Handbuch	*Handbuch* / Betriebsanleitung MAWIS-Security Die Betriebsanleitung beschreibt, wie MAWIS-Security für einen sicheren Betrieb zu betreiben ist. Die Bereitstellung erfolgt als PDF-Datei auf einem elektronischen Datenträger oder per Mail. Dateiname: 10-02-00416-DE_Betriebsanleitung_MAWISsecurity.pdf	Art-No. 10-02-00416 Version 5.0

* Erläuterung siehe *Information zur Versionierung*

Die ID-Tags werden dem Endbenutzer durch MOBA (Projektleitung) übergeben. Optional kann MOBA mit der Ausrüstung der Behälter mit den ID-Tags beauftragt werden. Im Rahmen eines solchen Auftrags erfolgen durch MOBA die Montage der ID-Tags an die Abfallbehälter sowie die Zuordnung der ID zum Verursacher.

MAWIS-MobilSecurity und MAWIS-OfficeSecurity werden dem Endbenutzer bei Übergabe des MAWIS-Systems vorinstalliert auf der jeweiligen Hardware bereitgestellt.

Information zur Versionierung

Die Versionsnummern setzen sich folgendermaßen zusammen: **x.y.d.f**

Teil	Beschreibung
x	***Major Version number*** (Hauptversionsnummer), wird bei Änderungen an EVG- Bestandteilen weitergezählt.
y	***Minor version number***, wird bei Änderungen an Nicht-EVG- Bestandteilen weitergezählt.
d	***Jahr (Zehner/Einer) und Kalenderwoche*** der ersten Release der x.y. Version.
f	***Zähler für Bug-fixes / kleine Änderungen*** ohne funktionelle Änderungen.

1.4.2.2 Logische Abgrenzung des EVG

Der EVG ist ein Produkt im Sinne der Common Criteria. Der EVG besteht aus dem *ID-Tag*, dem fahrzeugseitigen Sicherheitsmodul *MAWIS-MobilSecurity* und dem büroseitigen Sicherheitsmodul *MAWIS-OfficeSecurity*.

Alle anderen Komponenten (siehe auch Abbildung 1) sind nicht Teil des EVG, sondern der Umgebung des EVG.

Der EVG verfügt über eine externe Schnittstelle zu den Speichern des Fahrzeugcomputers, eine logische interne Schnittstelle zwischen dem ID-Tag und dem fahrzeugseitigen Sicherheitsmodul *MAWIS-MobilSecurity*, eine logische interne Schnittstelle zwischen dem fahrzeugseitigen Sicherheitsmodul *MAWIS-MobilSecurity* und dem büroseitigen Sicherheitsmodul *MAWIS-OfficeSecurity* und eine externe Schnittstelle zwischen *MAWIS-OfficeSecurity* und der Bürosoftware.

Die physischen Kanäle ID-Tag → fahrzeugseitiges Sicherheitsmodul sowie fahrzeugseitiges Sicherheitsmodul → büroseitiges Sicherheitsmodul sind nicht Bestandteil des EVG.

Weitere Schnittstellen, insbesondere die zu den Endverbrauchern (z.B. kommunalen Abrechnungsstellen), sind nicht Bestandteil des EVG. Die Bürosoftware und andere weiterverarbeitende Software sind ebenfalls nicht Bestandteil des EVG.

Um dem Leser der Sicherheitsvorgaben ein allgemeines Verständnis der Sicherheitsmerkmale des EVG zu vermitteln, werden folgend für jeden EVG-Teil die angebotenen logischen Sicherheitsmerkmale dargelegt.

ID-Tag

Im ID-Tag sind die Identifikationsdaten (AT1) des Abfallbehälters unveränderlich gespeichert (Read Only). Er versendet die Identifikationsdaten zusammen mit einem CRC-Prüfwert als Integritätsmerkmal an den Reader.

MAWIS-MobilSecurity

Das Sicherheitsmodul *MAWIS-MobilSecurity* überprüft die Integrität der Identifikationsdaten, indem es die CRC über die empfangenen Identifikationsdaten des ID-Tag bildet und mit dem ebenfalls empfangenen CRC-Prüfwert vergleicht. Ist die Integrität gegeben, versieht MAWIS-MobilSecurity den Leerungsdatensatz (AT) mit einem Schutz (Integritätsmerkmal), der gegen Veränderung des AT durch zufällige Manipulation wirkt und stellt den Leerungsdatensatz inklusive Integritätsmerkmal zur Übertragung an die Bürosoftware bereit. In die Bildung des Integritätsmerkmals wird die Fahrzeugkennung als Gültigkeitsmerkmal für den AT einbezogen.

Ist die Integrität nicht gegeben, werden die verfälschten Identifikationsdaten nicht weiterverarbeitet bzw. bereitgestellt.

Ein oder mehrere Leerungsdatensätze werden zu Leerungsdatenblöcken (AT+) zusammengefasst. *MAWIS-MobilSecurity* versieht die Leerungsdatenblöcke mit der eindeutigen Fahrzeugkennung sowie ebenfalls mit einem Schutz, der gegen Veränderung der Daten durch zufällige Manipulation wirkt.

Die Leerungsdatenblöcke werden zur Übertragung an den Bürorechner bereitgestellt und redundant in einem sekundären Speicher abgelegt.

MAWIS-OfficeSecurity

Das Sicherheitsmodul *MAWIS-OfficeSecurity* überprüft Integrität und Fahrzeugkennungen der empfangenen Leerungsdatenblöcke sowie der enthaltenen Leerungsdatensätze und speichert die Ergebnisse der Prüfung für jeden empfangenen Leerungsdatensatz bzw. Leerungsdatenblock im Datenbestand der MAWIScloudDB ab. Leerungsdatensätze, bei denen die Prüfung fehlschlug, werden als ungültig gekennzeichnet. Die Leerungsdatensätze, bei denen die Prüfung Übereinstimmung feststelle, sind integer und werden so gekennzeichnet. Die weiterverarbeitende Software kann diese Kennzeichnungen auswerten und entsprechend reagieren.

2 Postulate zur Übereinstimmung

Postulat der Übereinstimmung mit den CC

Die Sicherheitsvorgaben (Security Target - ST) und der EVG (Target of Evaluation - TOE) postulieren Übereinstimmung mit den

- Common Criteria for Information Technology Security Evaluation,
  Version 3.1, Revision 5

Die Sicherheitsvorgaben und der EVG sind CC Teil 2 erweitert (*CC part 2 extended*). Die Erweiterung besteht aus der Komponente

- FDP_ITT.5 “internal transfer integrity protection”

Die Sicherheitsvorgaben und der EVG sind CC Teil 3 konform (*CC Part 3 conformant*).

Die Sicherheitsvorgaben und der EVG erfüllen die Anforderungen der Vertrauenswürdigkeitsstufe *EAL1 augmented*. Die Anreicherung besteht aus den Komponenten:

- ASE_SPD.1 “security problem definition”
- ASE_OBJ.2 “security objectives” (ersetzt ASE_OBJ.1)
- ASE_REQ.2 “derived security requirements” (ersetzt ASE_REQ.1)

Postulat der Übereinstimmung mit Schutzprofilen und Begründungen

Die Sicherheitsvorgaben und der EVG sind konform zum Schutzprofil (PP conformant)

- BSI-PP-0010-2004,
  „Protection Profile Waste Bin Identification Systems (WBIS-PP)“,
  Version 1.04

Der EVG realisiert die gesamte Sicherheitsfunktionalität eines Abfall-Behälter-Identifikationssystems (Waste Bin Identification System – WBIS).

Die Angaben zur Art des EVG in Abschnitt 1.4 sind konsistent mit der Art des EVG im Schutzprofil WBIS-PP [4], Abschnitte 1.2 und 2 sowie 8.2 und 8.3.

Die Definition des Sicherheitsproblems in Abschnitt 3 dieser Sicherheitsvorgaben enthält alle Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken, wie im WBIS-PP [4], Abschnitte 3 und 8.4 definiert. Die Definition des Sicherheitsproblems im ST stimmt somit mit der im WBIS-PP überein. Begründung:

- Die Bedrohungen im ST wurden aus dem Schutzprofil WBIS-PP übernommen.
  T.Jam#1 wurde lediglich konkretisiert, um das Problem klarer darzustellen.
- Die Annahmen im ST wurden aus dem Schutzprofil WBIS-PP übernommen.
- Die organisatorischen Sicherheitspolitiken (OSPs) im ST (Abschnitt 3.2) wurden aus dem Schutzprofil übernommen (WBIS-PP, Abschnitt 3.3).

Bezüglich der Schutzwürdigen Objekte wurde aus der *Application Note 1* in WBIS folgende Ergänzung in dieses ST übernommen: Die Identifikationsdaten AT1 sind im ID-Tag gespeichert und bilden für sich ein schutzwürdiges Objekt bis zum Zeitpunkt der Bildung des Datensatzes AT.

Das ST enthält im Abschnitt 4.1 für den EVG alle Sicherheitsziele wie im Schutzprofil (WBIS-PP [4], Abschnitt 4.1) definiert.

Die Sicherheitsziele OT.Inv#1 und OT.Safe und die zugehörigen Abschnitte der Erklärung der Sicherheitsziele wurden konkretisiert, um sie an das konkretisierte Sicherheitsproblem anzupassen. Es wurden keine Sicherheitsziele hinzugefügt.

Zum Sicherheitsziel OT.Inv#1 enthält das Schutzprofil (WBIS-PP [4]) folgenden Anwendungshinweis:

Application Note 7: Anwendungshinweis 7:	The security objectives require only the recognition of for example missing data in ID-Tag. The TOE can optionally react by itself to such recognised events. Since this will be not realised in general it is left to the author of the Security Target to define in addition security objectives for the reaction to such events.	Die Sicherheitsziele erfordern lediglich die Erkennung beispielsweise fehlender Daten im ID-Tag. Auf solche erkannten Ereignisse kann der EVG optional selbstständig reagieren. Da dies in der Regel nicht umgesetzt wird, bleibt es dem Autor des Sicherheitsziels überlassen, zusätzlich Sicherheitsziele für die Reaktion auf solche Ereignisse zu definieren.

Der Hinweis wurde in diesen Sicherheitsvorgaben berücksichtigt. Für die Aufnahme zusätzlicher Sicherheitsziele besteht kein Bedarf.

Die Sicherheitsziele für die Einsatzumgebung im ST (Abschnitt 4.2) enthalten alle im Schutzprofil (WBIS-PP [4], Abschnitt 4.2) definierten Sicherheitsziele. In die Sicherheitsziele für die Einsatzumgebung in Abschnitt 4.2 dieses ST wurden als Detaillierung die Sicherheitsanforderungen an die (Nicht-) IT-Umgebung aus dem Schutzprofil (WBIS-PP [4], Abschnitt 5.4) übernommen.

Die Sicherheitsanforderungen sind konform zu den im PP angegebenen Sicherheitsanforderungen, da sie vom PP übernommen wurden.

3 Definition des Sicherheitsproblems

Der folgende Abschnitt dient der Definition von Art und Umfang der Sicherheitsbedürfnisse, die der EVG adressiert. Daher enthält dieser Abschnitt

(i) alle Annahmen an die Umgebung des EVG,
(ii) die zu schützenden Werte, die bekannten Angreifer und die Bedrohungen, die sie für die Werte darstellen sowie
(iii) die organisatorischen Sicherheitspolitiken oder Regeln, die der EVG erfüllen muss, um den Sicherheitsbedürfnissen zu genügen.

Im Folgenden werden zunächst die Werte, Subjekte und Angreifer definiert.

Schutzwürdige Objekte (Assets)

AT Ein Leerungsdatensatz AT zu einer Leerung ist ein schutzwürdiges Objekt. Ein Leerungsdatensatz AT besteht aus den Datenfeldern:

- AT1 Identifikationsdaten des Abfallbehälters
- AT2 Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.
- AT3 optional Wägeergebnis, wenn das Fahrzeug mit einem Wägesystem ausgestattet ist
- AT4 Zähler zur Prüfung der verlustfreien Übertragung von Leerungsdatensätzen

Die Identifikationsdaten AT1 sind im ID-Tag gespeichert und bilden für sich ein schutzwürdiges Objekt bis zum Zeitpunkt der Bildung des Datensatzes AT. Der Leerungsdatensatz AT kann optional Zusatzinformationen enthalten, wie z.B. Diagnosedaten, Zusatzeingaben sowie weitere, die jedoch keine schutzwürdigen Objekte darstellen.

AT+ Die Leerungsdatensätze AT werden vor der Übertragung von der Fahrzeugsoftware zum büroseitigen Sicherheitsmodul zu Freigabedatenblöcken AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt im WBIS bei der Übertragung zwischen Fahrzeugsoftware und büroseitigem Sicherheitsmodul.

Subjekte (Subjects)

S.Trusted Vertrauenswürdige Benutzer

Besatzung des Fahrzeugs, Benutzer des Bürorechners. Personen, die das System installieren oder warten. Ferner Personen, die für die Sicherheit der Umgebung verantwortlich sind.

Angreifer

S.Attack Angreifer

Eine Person oder ein für eine Person aktiver Prozess, die sich außerhalb des EVG befinden. Das Hauptziel des Angreifers S.Attack ist es, sensitive Daten der Anwendung zu modifizieren oder zu verfälschen. Der Angreifer verfügt höchstens über Kenntnisse offensichtlicher Schwachstellen.

3.1 Bedrohungen

Ein Angreifer nutzt die Schnittstellen des EVG mit dem Ziel, Schwachstellen auszunutzen. Dies führt zu einer zunächst nicht näher spezifizierten Kompromittierung der Sicherheit des EVG. Die Bedrohungen adressieren alle Werte.

Die im Schutzprofil WBIS-PP aufgeführte Bedrohung T.Jam#1 wurde konkretisiert.

T.Man Manipulierte Identifikationsdaten

Ein Angreifer (S.Attack) manipuliert die Identifizierungsdaten (AT1) im ID-Tag durch Mittel (z.B. mechanische Einwirkung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.

T.Jam#1 Gestörte Identifikationsdaten

Ein Angreifer (S.Attack) stört die Übertragung der Identifizierungsdaten (AT1) vom ID-Tag zum Reader im Fahrzeug oder vom Reader zur Fahrzeugsoftware durch Mittel (z.B. elektromagnetische Strahlung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.

T.Create Ungültige Leerungsdatensätze

Ein Angreifer (S.Attack) erzeugt beliebige Leerungsdatenblöcke (AT+) und überträgt diese an das Sicherheitsmodul.

T.Jam#2 Verfälschte Leerungsdatensätze

Ein Angreifer (S.Attack) verfälscht Leerungsdatensätze (AT) während der Bearbeitung und der Speicherung innerhalb des Fahrzeuges oder stört die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul z.B. durch elektromagnetische Strahlung, um die Daten der Leerungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen.

3.2 Organisatorische Sicherheitspolitik

Die folgende Regel wird für den EVG formuliert:

P.Safe Fehlertoleranz

Der EVG-Teil der Fahrzeugsoftware MAWIS-MobilSecurity muss sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Speicherung in einem sekundären Speicher so geschützt sind, dass die Übertragung der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul MAWIS-OfficeSecurity nach einem Verlust der Daten in einem primären Speicher möglich ist.

3.3 Annahmen

A.Id ID-Tag

Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert. Es werden nur ID-Tags mit eindeutigen Identifizierungsdaten installiert. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.

A.Trusted Vertrauenswürdiges Personal

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

A.Access Zugangsschutz

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

A.Check Überprüfung der Vollständigkeit

Der Nutzer (S.Trusted) prüft in regelmäßigen Intervallen, ob die von der Fahrzeugsoftware zum Sicherheitsmodul im Büro übertragenen Daten vollständig sind. Festgestellte Datenverluste werden durch wiederholte Datenübertragung behoben. Die Intervalle richten sich nach der Kapazität des entsprechenden Speichers des Fahrzeugcomputers.

A.Backup Datensicherung

Der Nutzer (S.Trusted) erstellt in regelmäßigen Intervallen Sicherungskopien der vom EVG erstellten Daten.

4 Sicherheitsziele

Die Sicherheitsziele bestimmen (entsprechend der gewünschten Sicherheitsstufe) die Fähigkeit des EVG, den Bedrohungen entgegenzuwirken und die organisatorischen Sicherheitspolitiken einzuhalten. Jedes Sicherheitsziel muss zurückzuführen sein auf

- die Aspekte der identifizierten zu begegnenden Bedrohungen
- die organisatorischen Sicherheitspolitiken, die der EVG erfüllen muss.

Die Sicherheitsziele sind als Unterstützung für den Leser gedacht. Sie bilden die Verbindung zwischen den identifizierten Sicherheitsbedürfnissen und den IT- Sicherheitsanforderungen.

4.1 Sicherheitsziele für den EVG

OT.Inv#1 **Erkennung ungültiger Identifikationsdaten**

Der EVG muss Manipulationen der im ID-Tag gespeicherten Identifikationsdaten (AT1) erkennen. Er muss auch Manipulationen erkennen, die im Fahrzeug während der Übertragung zwischen ID-Tag und Reader sowie vom Reader zur Fahrzeugsoftware stattfinden.

OT.Inv#2 **Erkennung ungültiger Leerungsdatenblöcke**

Der EVG muss jeglichen Versuch erkennen, willkürliche (d.h. ungültige) Leerungsdatenblöcke (AT+) an das Sicherheitsmodul zu übertragen. Der EVG muss Manipulationen an Leerungsdatensätzen (AT) während der Bearbeitung und Speicherung innerhalb des Fahrzeugs, und Manipulationen an Leerungsdatenblöcken (AT+) durch zufällige Störung während der Übertragung von der Fahrzeugsoftware zum Sicherheitsmodul erkennen.

OT.Safe **Fehlertoleranz**

Das Sicherheitsmodul MAWIS-MobileSecurity der Fahrzeugsoftware muss sicherstellen, dass die Leerungsdatenblöcke (AT+) durch redundante Speicherung in einem zweiten Speicher gesichert werden in der Art, dass im Falle eines Datenverlustes im Primärspeicher der Fahrzeugsoftware, eine Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul MAWIS-OfficeSecurity möglich ist.

4.2 Sicherheitsziele für die Umgebung

OE.Id **ID-Tag**

Der ID-Tag ist am Abfallbehälter befestigt. Im ID-Tag sind die Identifikationsdaten (AT1) des Abfallbehälters gespeichert. Es dürfen nur ID-Tags mit eindeutigen Identifikationsdaten verwendet werden. Die korrekte Zuordnung dieser Daten zur gebührenpflichtigen Person ist durch organisatorische Maßnahmen sicherzustellen, die nicht Gegenstand des EVG sind.

Detaillierung (R.Id)

Der Benutzer (S.Trusted) muss Folgendes sicherstellen:

Der ID-Tag ist am durch die Identifikationsdaten zu identifizierenden Abfallbehälter zu befestigen. Die Identifikationsdaten, die im ID-Tag gespeichert sind, müssen eindeutig sein. Durch organisatorische Mittel, die nicht Betrachtung des TOE sind, soll geleistet werden, dass die Verknüpfung zwischen Identifikationsdaten und gebührenpflichtiger Person hergestellt wird.

OE.Trusted **Vertrauenswürdiges Personal**

Es ist durch organisatorische Maßnahmen sicherzustellen, dass die Besatzung des Fahrzeuges sowie die Nutzer des Büro- PC (S.Trusted) autorisiert und vertrauenswürdig sind. Alle Personen, die das System installieren und warten, müssen autorisiert und vertrauenswürdig (S.Trusted) sein. Alle Personen, die für die Sicherheit der Umgebung des EVG zuständig sind, müssen autorisiert und vertrauenswürdig (S.Trusted) sein.

Detaillierung (R.Trusted):

Das Personal, durch das das Fahrzeug und das Sicherheitsmodul betrieben, installiert und gewartet wird, muss befugt und vertrauenswürdig sein. Alle für die Sicherheit der Umgebung verantwortlichen Personen sind befugt und vertrauenswürdig.

OE.Access **Zugangsschutz**

Die Umgebung muss durch geeignete Mittel (Verschluss, Zugangspasswörter etc.) sicherstellen, dass nur Nutzer oder Servicepersonal (S.Trusted) direkten Zugang zu den Komponenten des EVG hat- der ID-Tag ist davon ausgenommen. Die Manipulation der internen Kommunikationskanäle durch potenzielle Angreifer (S.Attack) innerhalb der IT- Struktur des Büro- PCs muss durch ausreichende Mittel ausgeschlossen werden.

Detaillierung (R.Access):

Die Umgebung muss durch geeignete Mittel sicherstellen, dass nur Nutzer und Service- Personal direkten Zugang zu den Komponenten des EVG haben (Ausnahme ist der ID-Tag). Die Umgebung soll jegliche Beeinflussung der internen Kommunikation innerhalb des Bürorechners verhindern.

OE.Check **Prüfen der Vollständigkeit**

Es ist sicherzustellen, dass der Nutzer (S.Trusted) in regelmäßigen Intervallen überprüft, ob die von der Fahrzeugsoftware zum Sicherheitsmodul im Büro transportierten Daten vollständig sind.

Festgestellter Datenverlust ist durch wiederholte Datenübertragung auszugleichen. Die Intervalle müssen mit der Kapazität des entsprechenden Speichers im Fahrzeugcomputer übereinstimmen.

Detaillierung (R.Check):

Der Benutzer (S.Trusted) soll in regelmäßigen Abständen die Vollständigkeit der Datenübertragung von Leerungsdatenblöcken (AT+) vom Fahrzeug zum Büro prüfen. Der Nutzer muss die Daten, von denen er festgestellt hat, dass sie nicht mit übertragen worden sind, erneut anfordern können, um sie wiederherzustellen. Die Intervalle von Prüfung und Wiederherstellung müssen passend zu dem Speicher sein, der auf dem Fahrzeugrechner zur Speicherung der Leerungsdatenblöcke (AT+) verfügbar ist.

OE.Backup Datensicherung

Es ist sicherzustellen, dass der Nutzer (S.Trusted) in regelmäßigen Intervallen Backup- Kopien der durch den EVG erzeugten Daten erstellt.

Detaillierung (R.Backup)

Der Nutzer muss die durch den EVG erzeugten Daten in regelmäßigen Abständen in geeignete Archive sichern.

4.3 Erklärung der Sicherheitsziele

4.3.1 Rückverfolgung der Sicherheitsziele

Die Tabelle zeigt die Beziehungen zwischen Sicherheitszielen einerseits und Bedrohungen, organisatorischen Sicherheitspolitiken sowie Annahmen andererseits.

Tabelle 5 Rückverfolgung der Sicherheitsziele

Sicherheitsziele / Bedrohungen Annahmen Politiken	OT.Inv#1	OT.Inv#2	OT.Safe	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup
T.Man	X							
T.Jam#1	X							
T.Create		X						
T.Jam#2		X						
A.Id				X				
A.Trusted					X			
A.Access						X		
A.Check							X	
A.Backup								X
P.Safe			X					

4.3.2 Wirksamkeit der Sicherheitsziele

4.3.2.1 Wirksamkeit bezüglich der organisatorischen Sicherheitspolitiken

P.Safe (Fehlertoleranz) etabliert die Verfügbarkeit der relevanten Daten für die Übertragung der Leerungsdatenblöcke (AT+) vom EVG-Teil MAWIS-MobilSecurity der Fahrzeugsoftware zum Sicherheitsmodul MAWIS-OfficeSecurity auch bei Verlust dieser Daten im primären Speicher der Fahrzeugsoftware, indem die Daten im sekundären Speicher gehalten werden. Dies wird vom Ziel OT.Safe genau wiederholt, sodass dieses Ziel für P.Safe ausreichend ist. Somit ist OT.Safe hinreichend zur Durchsetzung von P.Safe.

4.3.2.2 Wirksamkeit bezüglich der Bedrohungen

T.Man (Manipulierte Identifikationsdaten) behandelt Angriffe, durch die Identifikationsdaten (AT1) innerhalb des ID-Tag manipuliert werden. Gemäß OT.Inv#1 werden beschädigte Identifikationsdaten (AT1) durch den EVG erkannt (nachdem sie durch den ID-Tag-Reader gelesen und an die Fahrzeugsoftware übertragen wurden). Das wirkt der Bedrohung T.Man direkt entgegen. Damit ist OT.Inv#1 hinreichend wirksam gegen T.Man.

T.Jam#1 (Gestörte Identifikationsdaten) behandelt Angriffe, in denen (durch zufällige Störung) gestörte Identifikationsdaten (AT1) an den ID-Tag-Reader übergeben werden. Gemäß OT.Inv#1 werden beschädigte Identifikationsdaten (AT1) vom EVG erkannt (nachdem sie durch den ID-Tag-Reader gelesen und an die Fahrzeugsoftware übertragen wurden). Das wirkt der Bedrohung T.Jam#1 direkt entgegen. Damit ist OT.Inv#1 hinreichend wirksam gegen T.Jam#1.

T.Create (Ungültige Leerungsdatenblöcke) behandelt Angriffe, in denen willkürlich Leerungsdatenblöcke erstellt und dann an das Sicherheitsmodul übergeben werden. Gemäß OT.Inv#2 wird jeder Versuch erkannt, willkürliche (d.h. ungültige) Leerungsdatenblöcke an das Sicherheitsmodul zu übergeben. Das wirkt der Bedrohung T.Create direkt entgegen. Damit ist OT.Inv#2 hinreichend wirksam gegen T.Create.

T.Jam#2 (Verfälschte Leerungsdatensätze) richtet sich gegen Angriffe, bei denen Leerungsdatensätze (AT) während der Verarbeitung und Speicherung auf dem Fahrzeug beschädigt werden oder bei denen die Übertragung der Leerungsdatenblöcke zum Sicherheitsmodul gestört wird. Gemäß OT.Inv#2 werden Verfälschungen der Leerungsdatensätze (AT) während der Verarbeitung und Speicherung auf dem Fahrzeug und der Leerungsdatenblöcke während der Übertragung zum Sicherheitsmodul durch den EVG erkannt. Das wirkt der Bedrohung T.Jam#2 direkt entgegen. Damit ist OT.Inv#2 hinreichend wirksam gegen T.Jam#2.

4.3.2.3 Wirksamkeit bezüglich der Annahmen

A.Id (Identifikationseinheit) sichert, dass der ID-Tag an dem Abfallbehälter befestigt ist, den er identifiziert, sowie, dass die installierten ID-Tags eindeutig sind. Der Zusammenhang zwischen Identifikationsdaten und gebührenpflichtiger Person wird durch organisatorische Mittel erreicht. Da das Ziel OE.Id exakt das gleiche festlegt, ist dies hinreichend, A.Id aufrecht zu erhalten.

A.Trusted (Vertrauenswürdiges Personal) sichert, dass alle Subjekte (ausgenommen ein Angreifer) vertrauenswürdig sind. Da das Ziel OE.Trusted exakt das gleiche festlegt, ist dies hinreichend, A.Trusted aufrecht zu erhalten.

A.Access (Zugangsschutz) sichert, dass der Zugang auf den EVG auf vertrauenswürdiges Personal beschränkt ist (ausgenommen ist der ID-Tag). Er schließt ebenfalls aus, dass der Angreifer in der Lage ist, die internen Kommunikationskanäle innerhalb der IT- Struktur des Bürorechners zu beeinflussen. Da das Ziel OE.Access exakt das gleiche festlegt, ist dies hinreichend, A. Access aufrecht zu erhalten.

A.Check (Prüfung der Vollständigkeit) sichert, dass der Benutzer in regelmäßigen Abständen prüft, ob die vom Fahrzeug zum Büro transportierten Daten vollständig sind. Bei Festgestellung von Datenverlust werden die Daten durch wiederholte Übertragung wieder gewonnen. Die Abstände stimmen mit der Kapazität des entsprechenden Speichers auf dem Fahrzeugrechner überein. Da das Ziel OE.Check exakt das gleiche festlegt, ist dies hinreichend, A.Check aufrecht zu erhalten.

A.Backup (Datensicherung) sichert, dass der Benutzer in regelmäßigen Abständen Sicherheitskopien der durch den EVG erzeugten Daten macht, da der EVG keine entsprechende Funktionalität besitzt. Da das Ziel OE.Backup exakt das gleiche festlegt, ist dies hinreichend, A.Backup aufrecht zu erhalten.

5 Definition erweiterter Komponenten

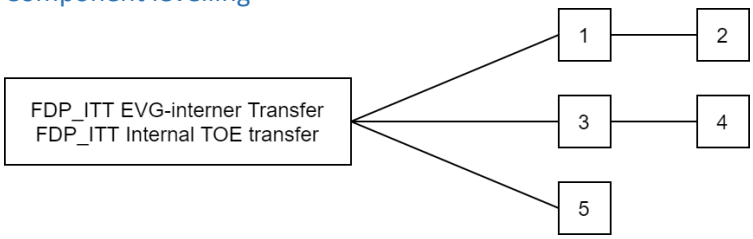
Es wurde beschlossen, FDP_ITT.5 explizit zu definieren, weil im Teil 2 der CC keine generischen funktionellen Sicherheitsanforderungen für den Schutz der Integrität von Anwenderdaten enthalten sind, wenn sie zwischen physikalisch voneinander getrennten Teilen des EVG übertragen werden. Weiterhin trifft FDP_ITT.5 die Erfordernisse besser als FDP_ITT.1, da es nicht notwendig erforderlich ist, dass der EVG Sicherheitspolitiken zur Zugriffskontrolle und/oder Sicherheitspolitiken zur Informationsflusskontrolle implementiert und nur auf die Manipulation von Daten zielt.

Die Definition von FDP_ITT.5 ist im Appendix C des Schutzprofils "Waste Bin Identification Systems (WBIS-PP)" [4] erfolgt und von dort entnommen:

Die Familie „Interner TOE-Transfer“ (FDP_ITT)“ wird wie folgt erweitert (hier werden nur Änderungen angegeben).

FDP_ITT Internal TOE transfer

Component levelling



FDP_ITT.5

Integritätsschutz des internen Transfers fordert den Schutz von Benutzerdaten gegen Manipulationen bei der Übertragung zwischen Teilen des EVG.	Internal transfer integrity protection requires user data to be protected against manipulations when transmitted between parts of the TOE.

Management: FDP_ITT.5

Es sind keine Managementaktivitäten vorgesehen.	There are no management activities foreseen.

Audit: FDP_ITT.5

Es sind keine auditierbaren Ereignisse vorgesehen	There are no auditable events foreseen.

FDP_ITT.5 Internal transfer integrity protection

Hierarchisch zu: keinen anderen Komponenten Abhängigkeiten: keine Abhängigkeiten	Hierarchical to: No other components. Dependencies: No dependencies

FDP_ITT.5.1

Die TSF müssen die [Zuweisung: SFPs für Integrität] durchsetzen, um die Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen physisch getrennten Teilen des EVG übertragen werden.	The TSF shall enforce the [assignment: integrity SFP(s)] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

6 IT- Sicherheitsanforderungen

Das Kapitel beschreibt die funktionellen Sicherheitsanforderungen sowie die Anforderungen an die Vertrauenswürdigkeit des EVG und der Umgebung.

Die funktionellen Sicherheitsanforderungen im Kapitel 6.1 sind den Common Criteria Teil 2 [2] entnommen (außer FDP_ITT.5 - dies ist in [4] definiert).

Die Anforderungen an die Vertrauenswürdigkeit in Kapitel 6.2 sind den Vertrauenswürdigkeitskomponenten der Common Criteria, Teil 3 [3] entnommen.

6.1 Funktionale Sicherheitsanforderungen an den EVG

Zuweisungen sind durch **Fettdruck** kenntlich gemacht.

6.1.1 Datenauthentisierung / Data authentication (FDP_DAU)

6.1.1.1 Einfache Datenauthentisierung / Basic data authentication (FDP_DAU.1)

FDP_DAU.1.1

Die TSF müssen die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von **Leerungsdatensätzen AT und Leerungsdatenblöcken AT+** bereitstellen.	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **records of clearance AT and clearance data blocks AT+**.

FDP_DAU.1.2

Die TSF müssen dem **Benutzer (S.Trusted)** die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angegebenen Information bereitstellen.	The TSF shall provide **user (S.Trusted)** with the ability to verify evidence of the validity of the indicated information.

6.1.2 EVG- interner Transfer / Internal TOE transfer (FDP_ITT)

6.1.2.1 Schutz der Integrität des internen Transfers / Internal transfer integrity protection (FDP_ITT.5)

FDP_ITT.5.1

Die TSF müssen die **Politik zur Datenintegrität** durchsetzen, um Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen physisch getrennten Teilen des TOE (EVG) übertragen werden.	The TSF shall enforce the **Data Integrity Policy** to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.
Für die Anforderung „Internal Transfer Integrity Protection (FDP_ITT.5)“ ist die folgende funktionale Sicherheitspolitik (SFP) **Politik zur Datenintegrität** definiert:	The following Security Function Policy (SFP) **Data Integrity Policy** is defined for the requirement “Internal transfer integrity protection (FDP_ITT.5)”:

Die Nutzerdaten (AT1 und AT+) sollen geschützt werden, um deren Integrität zu wahren.	The User Data (AT1 and AT+) shall be protected in order to maintain its integrity.

6.1.3 Integrität der gespeicherten Daten / Stored data integrity (FDP_SDI)

6.1.3.1 Überwachung der Integrität der gespeicherten Daten / Stored data integrity monitoring (FDP_SDI.1)

Dieser Abschnitt wurde angepasst an die in den CC 3.1 R5 formulierten Anforderungen:

FDP_SDI.1.1

Die TSF müssen die Benutzerdaten, die in von den TSF kontrollierten Containern gespeichert sind, auf **zufällige Manipulation** bei allen Objekten auf Basis folgender Attribute überwachen: **Identifikationsdaten AT1 innerhalb der Identifikationseinheit und Leerungsdatensätze AT während der Speicherung innerhalb des Fahrzeuges.**	The TSF shall monitor user data stored in containers controlled by the TSF for **random manipulation** on all objects, based on the following attributes: **identification data AT1 within identification unit and records of clearance AT during storage within the vehicle**.

6.1.4 Fehlertoleranz / Fault tolerance (FRU_FLT)

6.1.4.1 Verminderte Fehlertoleranz / Degraded fault tolerance (FRU_FLT.1)

FRU_FLT.1.1

Die TSF müssen den Betrieb **der Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im Sekundärspeicher gespeicherten Daten** sicherstellen, wenn die folgenden Fehler auftreten: **Verlust der Nutzerdaten im primären Speicher der Fahrzeugsoftware**.	The TSF shall ensure the operation of **the transfer of clearance data blocks (AT+) from the vehicle software to the security module with the aid of the data stored in secondary memory** when the following failures occur: **Loss of user data in the primary memory of the vehicle software**.

6.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Evaluierungsstufe ist EAL 1+.

In den Common Criteria, Part 3 [3] sind die für diese Evaluierungsstufe geforderten Vertrauenswürdigkeitsklassen und -komponenten formuliert. Sie sind in Tabelle 6 dargestellt. Über EAL1 hinaus wurde das ST um die Vertrauenswürdigkeitsklassen ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 angereichert. Diese Klassen sind hervorgehoben dargestellt.

Tabelle 6 Anforderungen an die Vertrauenswürdigkeitsstufe des EVG

Vertrauenswürdigkeitsklasse	**Vertrauenswürdigkeitskomponenten**	
ADV	ADV_FSP.1	Einfache funktionale Spezifikation Basic functional specification
AGD	AGD_OPE.1	Benutzerhandbuch, Betrieb Operational user guidance
	ADG_PRE.1	Vorbereitende Prozeduren Preparative procedures
ALC	ALC_CMC.1	Kennzeichnung des EVG Labelling of the TOE
	ALC_CMS.1	EVG-CM-Umfang TOE CM coverage
ASE	ASE_INT.1	ST-Einführung ST introduction
	ASE_CCL.1	Konformitätspostulate Conformance claims
	ASE_SPD.1	***Definition des Sicherheitsproblems*** ***Security problem definition***
	ASE_OBJ.2	***Sicherheitsziele*** ***Security objectives***
	ASE_ECD.1	Definition erweiterter Komponenten Extended components definition
	ASE_REQ.2	***Abgeleitete Sicherheitsanforderungen*** ***Derived security requirements***
	ASE_TSS.1	EVG-Übersichtsspezifikation TOE summary specification
ATE	ATE_IND.1	Unabhängiges Testen – Übereinstimmung Independent testing – conformance
AVA	AVA_VAN.1	Erfassung von Schwachstellen Vulnerability survey

6.3 Erklärung der Sicherheitsanforderungen

6.3.1 Begründung der Abhängigkeiten

Die Vertrauenswürdigkeitskomponenten entsprechen exakt der Spezifikation in EAL1. Alle Abhängigkeiten innerhalb der Komponenten von EAL1 sind somit vollständig erfüllt.

Durch die Ergänzung der Evaluierungsstufe um die Vertrauenswürdigkeitskomponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 entstehen weitere Abhängigkeiten.

Die Abhängigkeiten der funktionalen Anforderungen für den EVG und für die Umgebung sind nicht vollständig erfüllt. Folgende Tabelle zeigt die Abhängigkeiten und zeigt, wie sie erfüllt sind.

Tabelle 7 Abhängigkeiten der funktionalen Anforderungen

Anforderung	Abhängigkeiten	Erfüllt
ASE_SPD.1	Keine Abhängigkeiten	Nicht anwendbar
ASE_OBJ.2	ASE_SPD.1	Ja
ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	Ja Ja
FDP_DAU.1	Keine Abhängigkeiten	Ja, implizit
FDP_ITT.5	Keine Abhängigkeiten	Ja, implizit
FDP_SDI.1	Keine Abhängigkeiten	Ja, implizit
FRU_FLT.1	FPT_FLS.1	Siehe Diskussion unten

FRU_FLT.1 fordert vom EVG, dass der Datentransfer von der Fahrzeugsoftware zum Sicherheitsmodul gewährleistet ist, auch bei einem Datenverlust im primären Datenspeicher der Fahrzeugsoftware. Diese Anforderung dient der Erfüllung der organisatorischen Sicherheitspolitiken, die sich eher auf die Verfügbarkeit der Daten als auf die korrekte Funktion der Software bzw. beziehen. Sie beziehen sich auch nicht auf einen sicheren Zustand der Software im Sinne der Bedrohungen, die der EVG abwehren soll. Da sich die abhängige Komponente FPT_FLS.1 mehr auf einen sicheren Zustand des EVG (z.B. seiner Software) bezieht, ist sie nicht für den EVG anwendbar.

6.3.2 Abdeckung der Sicherheitsanforderungen

Tabelle 8 Zuordnung der funktionalen Sicherheitsanforderungen zu den Sicherheitszielen des EVG

Sicherheitsziele / Funktionale Sicherheits-anforderungen	OT.Inv#1	OT.Inv#2	OT.Safe
FDP_DAU.1		X	
FDP_ITT.5	X	X	
FDP_SDI.1	X	X	
FRU_FLT.1			X

6.3.3 Zulänglichkeit der Sicherheitsanforderungen zur Erfüllung der Sicherheitsziele

6.3.3.1 Zulänglichkeit der EVG- Sicherheitsanforderungen und gegenseitige Unterstützung

OT.Inv#1 (Erkennung gestörter Identifikationsdaten) zielt auf die Erkennung der Manipulation von Identifikationsdaten (AT1) innerhalb der ID-Tags und während der Übertragung zwischen ID-Tag und dem Sicherheitsmodul MAWIS-MobilSecurity, welche getrennte Teile des EVG darstellen. Der Schutz der Integrität der im ID-Tag gespeicherten Identifikationsdaten (AT1) wird durch FDP_SDI.1 gefordert und begegnet direkt der zufälligen Verfälschung dieser Daten. Der Schutz der Anwenderdaten AT1, um ihre Integrität zu sichern, ist in FDP_ITT.5 für die Übertragung von Daten zwischen physisch voneinander getrennten Teilen des EVG gefordert. Die Integrität der Daten zu sichern, schützt direkt gegen Manipulation der Daten während der Übertragung.

OT.Inv#2 (Erkennung ungültiger Datenblöcke) zielt auf die Erkennung der Manipulation von Leerungsdatenblöcken (AT+), die zwischen der Fahrzeugsoftware und dem Sicherheitsmodul übertragen werden, bei denen es sich um physisch getrennte Teile des EVG handelt. Der Schutz der Benutzerdaten AT+ zur Gewährleistung ihrer Integrität, ist durch FDP_ITT.5 für die Übertragung von Daten zwischen physisch getrennten Teilen des EVG gefordert. Die Gewährleistung der Datenintegrität schützt unmittelbar vor Manipulationen der Daten. OT.Inv#2 zielt auch auf die Erkennung ungültiger Leerungsdatensätze (AT) während der Verarbeitung und Speicherung im Fahrzeug und auf Manipulationen von Leerungsdatenblöcken AT+, die zum Sicherheitsmodul übertragen werden. Der EVG hat gemäß FDP_DAU.1 die Fähigkeit, Nachweise zu erzeugen, die der Benutzer verwenden kann, die Gültigkeit der Daten zu überprüfen. Der Schutz der Integrität der im Fahrzeug gespeicherten Benutzerdaten (AT) wird durch FDP_SDI.1 gefordert und begegnet direkt zufälligen Manipulationen dieser Daten. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig für die Datenauthentizität und -integrität. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 decken somit das Sicherheitsziel OT.Inv#2 ausreichend ab.

OT.Safe (Fehlertoleranz) zielt auf die Verfügbarkeit der für die Übertragung der Leerungsdatenblöcke (AT+) vom Sicherheitsmodul MAWIS-MobilSecurity als Teil der Fahrzeugsoftware zum Sicherheitsmodul MAWIS-OfficeSecurity relevanten Daten auch für den Fall eines Datenverlustes im primären Datenspeicher der Fahrzeugsoftware. Die Durchführung dieses Datentransfers mit Hilfe eines sekundären Datenspeichers nach dem Verlust der Daten im Primärdatenspeicher wird durch den EVG gemäß FRU_FLT.1 realisiert.

6.3.4 Erklärungen zur Wahl der Sicherheitsanforderungen

Die Vertrauenswürdigkeitsstufe für den EVG ist EAL1 *augmented*, angereichert um die Vertrauenswürdigkeitskomponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2. Diese angereicherte Vertrauenswürdigkeitsstufe bietet einen bedeutenden Zuwachs der Sicherheit gegenüber einem nicht evaluierten IT-Produkt oder -System, indem Vertrauen in den korrekten Betrieb geschaffen wird, während die Bedrohungen der Sicherheit als nicht schwerwiegend angesehen werden, was direkt mit den eher niedrigen durch den EVG zu schützenden Werten zusammenhängt.

EAL1 mit der gewählten Anreicherung bietet unabhängige Vertrauenswürdigkeit, indem es die Annahme unterstützt, dass beim Schutz der in den Leerungsdatensätzen enthaltenen Informationen die gebotene Sorgfalt angewendet wurde und dass der EVG entsprechend des Kundenwunsches einen nützlichen Schutz vor den identifizierten Bedrohungen bietet.

Durch EAL1 mit oben genannten Anreicherungen wird der EVG bewertet, wie er dem Kunden zur Verfügung gestellt wird, einschließlich unabhängiger Tests gegen eine Spezifikation sowie der Prüfung der bereitgestellten Benutzerdokumentation.

Es ist vorgesehen, dass eine EAL1-Evaluation ohne Unterstützung durch den Entwickler des EVG und mit minimalem Aufwand erfolgreich durchgeführt werden kann. Dies ermöglicht die erforderliche Flexibilität bei der Zusammenstellung des Systems aus aktuell am Markt verfügbaren Modulen und hält die damit verbundenen Kosten für die Evaluation auf einem angemessen niedrigen Niveau.

Die Anreicherung von EAL1 um die oben genannten Komponenten wurde vorgenommen, um eine angemessene Prüfung der in Abschnitt 3 definierten Problemdefinition des EVG und der darauf aufbauenden Sicherheitsziele und Anforderungen durchzuführen, welche bei EAL1 noch nicht gefordert ist.

7 EVG-Übersichtsspezifikation

7.1 EVG-Sicherheitsfunktionen

7.1.1 TSF_TagID_Check

TSF_TagID_Check prüft die AT1, indem die CRC über die vom ID-Tag empfangenen Daten AT1 berechnet und mit dem ebenfalls empfangenen CRC-Prüfwert verglichen wird. Ergebnis der Prüfung ist die Information, ob die berechnete CRC mit der vom ID-Tag empfangenen übereinstimmt.

7.1.2 TSF_GenerateAT_Check

Die Funktion generiert einen Nachweis, der als Garantie für die Gültigkeit eines Leerungsdatensatzes verwendet werden kann, indem eine Fahrzeugkennung erzeugt wird.

Die Funktion generiert einen Nachweis, der als Garantie für die Vollständigkeit übertragener Datensätze verwendet werden kann, indem ein fortlaufender Zählwert erzeugt und dem AT hinzugefügt wird.

Es wird ein CRC-Prüfwert über den AT sowie über die Fahrzeugkennung berechnet.

Der CRC-Prüfwert wird an den Aufrufer zurückgegeben und muss gemeinsam mit den Daten AT übertragen werden, damit dessen Integrität und Gültigkeit nachgewiesen werden können.

7.1.3 TSF_GenerateATPlus_Check

Die Funktion generiert einen Nachweis, der als Garantie für die Gültigkeit eines Leerungsdatenblockes AT+ verwendet werden kann, indem eine Fahrzeugkennung erzeugt und dem AT+ hinzugefügt wird.

Es wird ein CRC-Prüfwert über den AT+ berechnet.

Der CRC-Prüfwert wird an den Aufrufer zurückgegeben und muss gemeinsam mit den Daten AT+ übertragen werden, damit deren Integrität nachgewiesen werden kann und damit die Fahrzeugkennung als Garantie für die Gültigkeit des AT+ verwendet werden kann.

7.1.4 TSF_Store_ATPlus

Die Funktion bewirkt, dass ein gesicherter Leerungsdatenblock AT+ redundant auf dem Fahrzeugrechner im sekundären Datenspeicher gespeichert wird. Leerungsdatenblöcke werden mindestens 2 Monate[3] im sekundären Datenspeicher vorgehalten und können innerhalb dieses Zeitraumes wiederholt übertragen werden.

Die Funktion bewirkt auch, dass die gesicherten Leerungsdatensätze AT redundant auf dem Fahrzeugrechner im sekundären Datenspeicher gespeichert werden.

[3] gilt für unterstellte tägliche Leerung von 3000 Behältern an einem Fahrzeug

7.1.5 TSF_Check_ATPlus

Die Funktion berechnet einen CRC-Prüfwert über den an das Sicherheitsmodul übergebenen Leerungsdatenblock AT+.

Der berechnete CRC-Prüfwert wird mit dem an das Sicherheitsmodul übergebenen CRC-Prüfwert des AT+ verglichen.

Weiterhin wird geprüft, ob die im Leerungsdatenblock AT+ enthaltene Fahrzeugkennung gültig ist.Das Ergebnis (gültig/ungültig) wird angezeigt, dabei handelt es sich um die Information, die aus dem Vergleich resultiert und angibt, ob der an den EVG übergebene Leerungsdatenblock AT+ vollständig und korrekt ist und ob eine gültige Fahrzeugkennung für den Leerungsdatenblock AT+ vorliegt. Die aus dem Vergleich resultierende Information wird vom Sicherheitsmodul für die Weiterverarbeitung genutzt.

7.1.6 TSF_Check_AT

Die Funktion berechnet einen CRC-Prüfwert. Die Bildung erfolgt über den an das Sicherheitsmodul übergebenen Leerungsdatensatz AT sowie die im AT+ enthaltene Fahrzeugkennung.

Der berechnete CRC-Prüfwert wird mit dem an das Sicherheitsmodul übergebenen CRC-Prüfwert des AT verglichen.

Das Ergebnis (gültig/ungültig) wird angezeigt, dabei handelt es sich um die Information, die aus dem Vergleich resultiert und angibt, ob der an den EVG übergebene Leerungsdatensatz AT vollständig und korrekt ist und ob eine gültige Fahrzeugkennung für den Leerungsdatensatz AT vorliegt. Die aus dem Vergleich resultierende Information wird vom Sicherheitsmodul für die Weiterverarbeitung genutzt.

7.2 Zusammenwirken der Sicherheitsfunktionen

Tabelle 9 Gegenüberstellung funktioneller Sicherheitsanforderungen und Sicherheitsfunktionen des EVG

Sicherheitsfunktion / Funktionelle Sicherheits-anforderungen	TSF_TagID_Check	TSF_GenerateAT_Check	TSF_GenerateATPlus_Check	TSF_Store_ATPlus	TSF_Check_ATPlus	TSF_Check_AT
FDP_DAU.1		x	x		x	x
FDP_ITT.5	x	x	x		x	x
FDP_SDI.1	x	x				x
FRU_FLT.1				x		

FDP_DAU.1 ist erfüllt,

- weil durch die Funktion TSF_GenerateAT_Check der Nachweis für die Gültigkeit eines Leerungsdatensatzes AT generiert wird.
- weil durch die Funktion TSF_GenerateATPlus_Check der Nachweis für die Gültigkeit eines Leerungsdatenblockes AT+ generiert wird.
- weil der Benutzer durch die Funktion TSF_Check_AT die Fähigkeit zur Verifizierung des Gültigkeitsnachweises für einen Leerungsdatensatz AT erhält.
- weil der Benutzer durch die Funktion TSF_Check_ATPlus die Fähigkeit zur Verifizierung des Gültigkeitsnachweises für einen Leerungsdatenblock AT+ erhält.

FDP_ITT.5 ist erfüllt,

- weil durch TSF_TagID_Check die Integrität der vom ID-Tag empfangene Daten AT1 überprüft wird, die zwischen den materiell getrennten EVG- Teilen ID-Tag und Fahrzeugsoftware übertragen werden. Dies ist möglich, weil nur ID-Tags mit CRC verwendet werden.
- weil durch TSF_GenerateAT_Check und TSF_GenerateATPlus_Check die Voraussetzung dafür geschaffen wird, dass die Integrität von Leerungsdatensätzen AT und Leerungsdatenblöcken AT+ geprüft werden kann.
- weil durch die Funktion TSF_Check_AT die Prüfung der Integrität eines Leerungsdatensatzes AT realisiert wird.
- weil durch die Funktion TSF_Check_ATPlus die Prüfung der Integrität eines Leerungsdatenblockes AT+ realisiert wird. Nur vollständige Leerungsdatenblöcke AT+ mit korrekten Leerungsdatensätzen AT werden weiterverarbeitet.

FDP_SDI.1 ist erfüllt,

- weil TSF_TagID_Check die Identifikationsdaten AT1 nach dem Empfang durch die Fahrzeugsoftware anhand der mit den Identifikationsdaten mit gesendeten CRC prüft. Nur unverfälschte AT1 werden weiterverarbeitet.
- weil vor der Speicherung von AT innerhalb des Fahrzeuges TSF_GenerateAT_Check die Voraussetzung schafft, dass zufällige Manipulationen während der Speicherung innerhalb des Fahrzeuges entdeckt werden können.
- Weil TSF_Check_AT nach der Übertragung von AT vom Fahrzeug die AT auf zufällige Manipulation überprüft.

FRU_FLT.1 ist erfüllt, weil durch TSF_Store_ATPlus Leerungsdatenblöcke (AT+) redundant im sekundären Datenspeicher des Bordrechners gespeichert werden. Dies ist die Voraussetzung dafür, dass es dem Benutzer möglich ist, Leerungsdatenblöcke (AT+) erneut von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im Sekundärspeicher gespeicherten Daten zu übertragen, falls Nutzerdaten im primären Speicher der Fahrzeugsoftware verloren gegangen sind. FRU_FLT.1 ist außerdem erfüllt, weil durch TSF_Store_ATPlus Leerungsdatensätze (AT) redundant im sekundären Datenspeicher des Bordrechners gespeichert werden. Dies ist die Voraussetzung dafür, dass bei einem Verlust von Nutzerdaten im primären Datenspeicher während der Speicherung auf dem Fahrzeugrechner, auf die Daten im sekundären Datenspeicher zurückgegriffen werden kann.

Die Aufstellung zeigt, dass die Sicherheitsfunktionen zusammenwirken, sich gegenseitig unterstützen und somit die funktionalen Anforderungen erfüllen.

8 Quellen

[1] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model
April 2017; Version 3.1, Revision 5, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional components
April 2017; Version 3.1, Revision 5, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance components
April 2017; Version 3.1, Revision 5, CCMB-2017-04-003.

[4] Protection Profile, Waste Bin Identification Systems WBIS-PP
Version 1.04,
Bundesamt für Sicherheit in der Informationstechnik
(BSI-PP-0010-2004)

[5] CAN Specification
Version 2.0
1991, Robert Bosch GmbH, Postfach 30 02 40, D-70442 Stuttgart

9 Anhang 1: Transponder Übersicht

Dieser Anhang erläutert die technischen Kernparameter sowie die Bezeichnungen der Transpondertypen, die zur Herstellung des Identifikationssystems MAWIS-Security, Rev. 4.0 zugelassen sind.

Es werden Transponder eingesetzt, die den in der DIN 30745 spezifizierten technischen Anforderungen entsprechen.

Eingesetzt werden Transponder, deren Unique ID und CRC-Prüfwert im Read-Only Teil des Transponders gespeichert sind.

Tabelle 10 Liste der ID-Tags

ID-Tag (Hersteller)	**Chip-Spezifikation**
TRPGR30ENATGA TRPGR30ENATGB (Texas Instruments)	Protokoll entsprechend ISO 11785 , Half duplex system (HDX) 80-Bit Read-Only Type, Codestruktur entsprechend DIN EN 14803
EM4205/EM4305 (EM Microelectronic)	Protokoll entsprechend ISO 11785 , Full duplex system (FDX) Programmiert zu 80-Bit Read-Only Type, Codestruktur entsprechend DIN EN 14803
SIC279 (Silicon Craft)	Protokoll entsprechend ISO 11785, Half duplex system (HDX) Programmiert zu 80-Bit Read-Only Type, Codestruktur entsprechend DIN EN 14803
Impinj Monza 4QT (Impinj)	ISO/IEC 18000-63 (UHF) 860…960MHz Programmiert zu Read-Only Type, Codestruktur entsprechend DIN 30745
UCODE G2iM+ (NXP)	ISO/IEC 18000-63 (UHF) 860…960MHz Programmiert zu Read-Only Type, Codestruktur entsprechend DIN 30745