MAWIS, Rev. 3.0

Sicherheitsvorgaben für die Zertifizierung nach WBIS PP

BSI-DSZ-CC-0496

Version 34

erstellt von: Stephan Holz
erreichbar unter: s.holz@moba.de
Stand: 28.04.08
zuletzt geändert von: Stephan Holz

Inhaltsverzeichnis

Glossar

Tabelle 1: Begriffserklärungen

Begriff / Abkürzung	Erklärung
Identification Unit	ID- Tag oder Transponder, der die Identifikationsdaten eines Müllbehälters trägt. Er ist am Müllbehälter (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 des Fahrzeugrechners der Firma MOBA Mobile Automation AG

1 ST- Einführung

Dieses Security Target beschreibt die Vorgaben für das Behälteridentifikationssystem MAWIS für die Zertifizierung des Produktes nach Common Criteria for Information Technology ([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 schwarzer Schrift gehalten. Neu in die Vorgaben aufgenommene Texte sind an ihrer grauen Schrift erkennbar.

1.1 ST- Identifikation

Titel: MAWIS Rev. 3.0 - Sicherheitsvorgaben nach WBIS
Autor: Stephan Holz
MOBA Mobile Automation AG

ST- Version: 34
ST- Datum: 28.04.08

1.2 ST- Übersicht

Das MAWIS ist ein System, durch das Abfallbehälter mit einem ID- Tag (mit elektronischen Chip, dem Transponder) identifiziert werden, um feststellen zu können, wie oft der einzelne Abfallbehälter geleert worden ist. Dabei handelt es sich bei diesem System nicht um die direkte Identifizierung von Abfällen, sondern um die Identifizierung der Behälter, in denen Abfälle zur Entsorgung bereitgestellt werden.

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

Häufig wird das System auch mit zum Beispiel einem optionalen Wiege- oder einem Volumenmesssystem kombiniert, um die Entsorgungsleistungen nach Häufigkeit und nach Gewicht 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.

Das Abfall-Behälter-Identifikations-System MAWIS basiert 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. Daher werden die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vor Manipulation und Verlust geschützt.

Nach Abschluss einer Leerungstour des Fahrzeuges werden alle gesammelten Daten in das Büro des Betriebshofes (kommunal oder privat) mit unterschiedlichen Medien (Datenträger, Kabel, drahtlos) übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Von hieraus können diese Daten regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet oder direkt von Abrechnungssoftware verwendet werden.

1.3 Postulat der Übereinstimmung mit den CC

Common Criteria for Information Technology Security Evaluation, Version 2.3, CCMB-2005-08 (ISO 15408:2005), August 2005

Common Evaluation Methodology for Information Technology Security Evaluation, Version 2.3, CCMB-2005-08-004 (ISO 15408:2005), August 2005

Der EVG ist Teil 2 erweitert.

Der EVG ist Teil 3 konform und erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL1. Der EVG ist konform zum Schutzprofil "Waste Bin Identification Systems (WBIS-PP)", Version 1.04.

2 EVG-Beschreibung

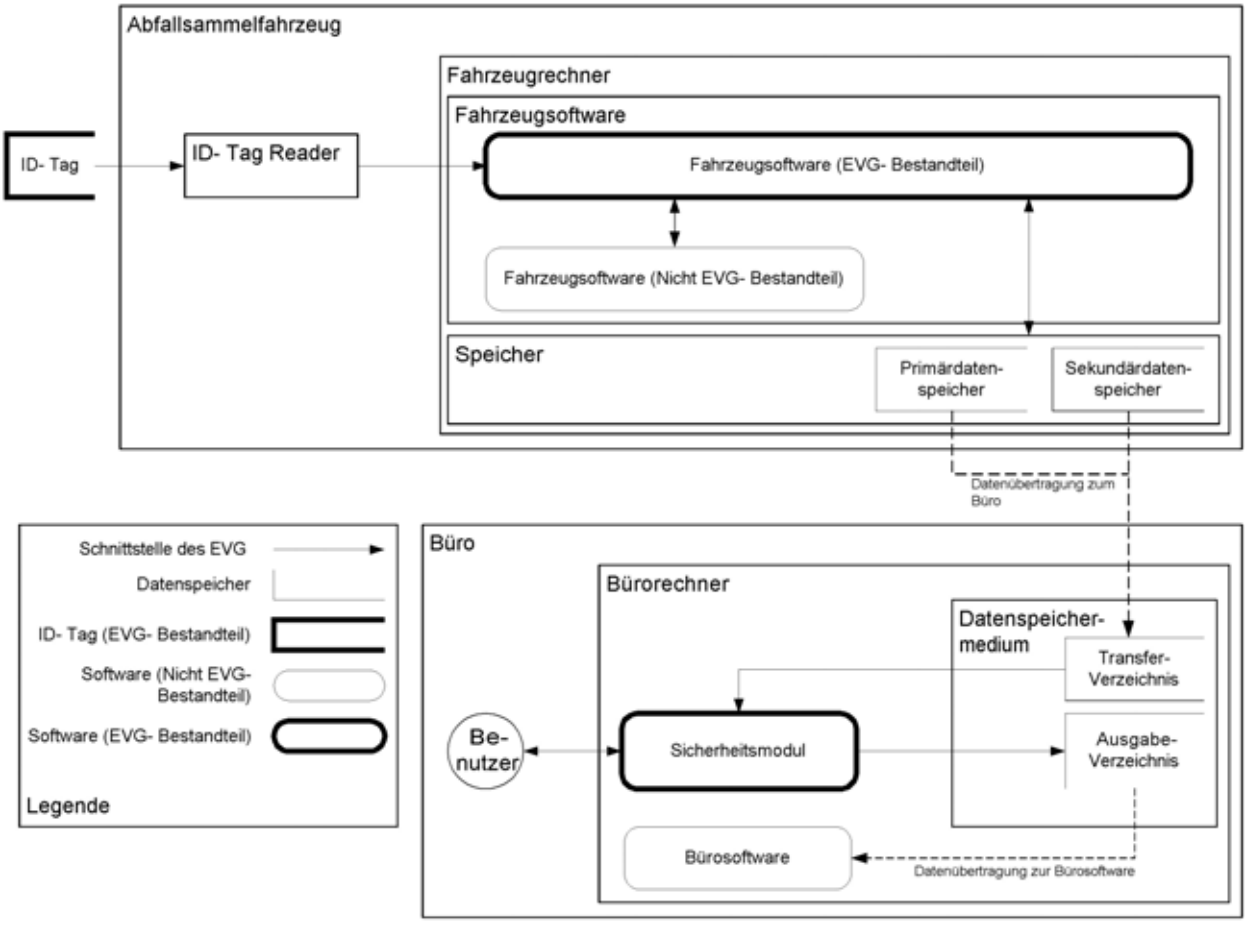
2.1 Überblick

Das Abfallbehälter- Identifizierungssystem (WBIS) besteht aus folgenden Komponenten:

- ID- Tag mit den Identifizierungsdaten des Abfallbehälters
- Fahrzeug mit dem (ID- Tag-) Reader (Ident-Control), Fahrzeugrechner (MOBA Operand oder kompatibel) und einem optionalem Wiege-, Volumenmess- oder ähnlichem System. Die Fahrzeugsoftware ist auf dem Fahrzeugrechner installiert.
- Bürorechner im Büro. Das Sicherheitsmodul und die Bürosoftware sind auf dem Bürorechner installiert.

Die folgende Abbildung gibt einen Überblick über das Abfallbehälter- Identifizierungssystem MAWIS

Abbildung 1 Überblick MAWIS- Komponenten



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 Identifikationsdaten beim Hersteller programmiert werden und danach nicht wieder modifiziert werden können (Read Only-Transponder). Darüber hinaus enthalten die zum Einsatz kommenden Transponder eine CRC-Prüfsumme, die über die Identifikationsnummer gebildet und durch den ID- Tag mit den Identifikationsdaten versendet wird. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während der Leerung eines Abfallbehälters durch den 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.

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 in einer gesicherten Archivdatei zur Übertragung zum Bürorechner bereitgestellt. Optional kann die Archivdatei zusätzliche Informationen enthalten. Dazu gehören beispielsweise die während der Entleerungen von einer Waage ermittelten Abfallgewichte. Die Archivdatei wird vom Abfallsammelfahrzeug zum Bürorechner übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Die Übertragung kann über unterschiedliche Medien (Datenträger, Kabel, drahtlos) erfolgen. Übertragungsstrecke und –verfahren gehören nicht zum EVG. Die optionalen Informationen werden ebenfalls nicht vom EVG betrachtet.

Die die Leerungsdatenblöcke enthaltenden Archivdateien 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 im sekundären Datenspeicher vorgehalten und können innerhalb dieses Zeitraumes wiederholt übertragen werden.

Bei der Übermittlung der Leerungsdatenblöcke an die Bürosoftware wird durch das Sicherheitsmodul sichergestellt, dass nur die in einem Fahrzeug erstellten Datenblöcke als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt, indem

übertragene Archivdateien durch das Sicherheitsmodul im Bürorechner auf Vollständigkeit, Integrität und Authentizität untersucht werden. Gültige und integere Leerungsdatensätze und Leerungsdatenblöcke werden weiterverarbeitenden Systemen in Form der Archivdateien zur Verfügung gestellt und können regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

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 Angriffpotential 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.

Folgende Funktionen werden durch den EVG realisiert:

- Sicherung der Identifikationsdaten des Abfallbehälters im ID- Tag und Versenden der Identifikationsdaten an den Reader
- Entgegennehmen der Identifikationsdaten vom Reader
- Prüfen der CRC- Checksumme der ID- Tags
- Bei erfolgreicher Prüfung bilden eines Leerungsdatensatzes aus den Identifikationsdaten des Abfallbehälters und dem Zeitstempel des Leerungsvorgangs. (und ggf. weiterer Daten)
- Sichern des Leerungsdatensatzes durch ein Integritäts- und Gültigkeitsmerkmal
- Speichern der geschützten Leerungsdatensätze
- Bilden eines Leerungsdatenblockes
- Sichern des Leerungsdatenblockes durch ein Integritäts- und Gültigkeitsmerkmal
- Speichern der geschützten Leerungsdatenblockes
- Redundantes Speichern der Daten, sodass ein Übertragen der Leerungsdatenblöcke auch nach einem Verlust der Daten im Primärspeicher möglich ist.
- Im Sicherheitsmodul prüfen der übertragenen Leerungsdatenblöcke und Leerungsdatensätze auf Gültigkeit und Integrität
- Anzeigen des Ergebnisses der Prüfung

2.2 Lieferumfang

Tabelle 2: MAWIS- Systemkomponenten

Komponente	Typ / Bezeichnung	Version	EVG-Bestand-teil
Transponder (ID- Tag)	Hardware / Transponder	Siehe Anhang 1	Ja
Reader	Hardware	Ab Version 2.0	Nein
Fahrzeugrechner	Hardware / MOBA Operand oder kompatible	Ab Version 3.0	Nein
Firmware- Ident-Control	Software	Ab Version 9.5.30 (für IDC HW- Versi-on 2.0)	Nein
	Software	Ab Version 2.0.0.0 (für IDC HW- Versi-on 3.0)	Nein
Fahrzeugsoftware	Software / MAWISMobil.exe	Ab Version *1.6.812.0*	Nein
	Software / MAWISMobilSecurity.dll	1.0.812.1	Ja
Sicherheitsmodul	Software / MawisSecurity.exe	1.0.808.1	Ja
Dokumentation	Systemverwalterhandbuch / „Systemverwalterhandbuch“	10	Ja
Dokumentation	Systemverwalterhandbuch und Be-dienungsanleitung / „Beschreibung der Anwendung MAWISSecurity.exe“	9	Ja
Dokumentation	Bedienungsanleitung / „Handbuch MAWIS Software MA-WISMobil“	18	teilweise
Dokumentation	Systemverwalterhandbuch / „Handbuch Wartung MAWISMobil“	6	Ja

2.3 System- Voraussetzungen zum Betrieb der Komponenten

Tabelle 3: Hardware- Voraussetzungen

Komponenten	Voraussetzungen	
MAWISMobil.exe MAWISMobilSecurity.DLL	Fahrzeugrechner mit Betriebssystem: Filesystem: IO- Komponenten: 	 WinCE ab Version 5.0 Flash- Filesystem mindestens 32MByte RAM- Filesystem mindestens 64MByte Farbiges TFT Display, Format 16:9 mindes-tens 400 x 240 pixel Touch Screen,

Komponenten	Voraussetzungen	
		Lautsprecher mindestens 1x CAN USB- Interface zum Zugriff auf Memory-Sticks
	externer Speicher:	Datenspeicher mindestens 128KByte
MAWISSecurity.EXE	PC mit:	
	Betriebssystem:	mind. Windows XP
	.NET	.NET- Framework Version 1.0
	Speicher:	Festplatte oder Netzwerkspeicher mit mindestens 500MB freier Kapazität.
	IO- Komponenten:	USB- Interface zum Zugriff auf Memory-Sticks Maus Tastatur Bildschirm

2.4 Abgrenzung des Evaluierungsgegenstandes

Der Evaluierungsgegenstand ist ein Produkt im Sinne der Common Criteria. Der Evaluierungsgegenstand besteht aus dem ID- Tag, einem Teil der Fahrzeugsoftware und den Sicherheitsmodulen. Alle anderen Komponenten (siehe auch Abbildung 1 Überblick MAWIS- Komponenten) sind nicht Bestandteil des Evaluierungsgegenstands und gehören zu dessen Umgebung.

2.4.1 Schnittstellen des EVG

Externe Schnittstellen sind die Schnittstellen, an denen Daten durch den EVG ausgegeben bzw. übernommen werden.

Der EVG besitzt folgende externe Schnittstellen:

INT1 Eine unidirektionale Schnittstelle zwischen dem ID-Tag und dem ID-Tag- Reader. Sie ist unidirektional, da nur Daten vom ID-Tag zum ID-Tag- Reader übertragen werden.

INT2 Eine unidirektionale Schnittstelle zwischen den ID-Tag- Readern und dem EVG-Teil der Fahrzeugsoftware. Sie ist unidirektional, da die ID-Tag- Reader Daten über den CAN-Bus an den EVG-Teil der Fahrzeugsoftware schicken.

INT3 Eine bidirektionale Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem Nicht-EVG-Teil der Fahrzeugsoftware. Sie ist bidirektional, weil gesicherte Leerungsdatensätze AT, Leerungsdatenblöcke AT+ sowie optionale Daten zwischen den beiden Teilen ausgetauscht werden.

INT4 Eine bidirektionale Schnittstelle zwischen EVG-Teil der Fahrzeugsoftware und dem primären und sekundären Datenspeichern. Sie ist bidirektional, da gesicherte Leerungsdatenblöcke AT+ auf die externen Speicher übertragen, wieder gelesen bzw. gelöscht werden.

INT5 Eine unidirektionale Schnittstelle zwischen einem oder zwei externen Transferverzeichnissen und dem Sicherheitsmodul. Sie ist unidirektional, da das Sicherheitsmodul gültige Leerungsdatenblöcke (AT+) aus dem Transferverzeichnis verschiebt.

INT6 Eine bidirektionale Schnittstelle zwischen dem Sicherheitsmodul und dem Benutzer. Sie ist bidirektional, da das Sicherheitsmodul den Benutzer über Fehler bei der Prüfung eines Leerungsdatenblockes (AT+) bzw. bei der Nutzung des Sicherheitsmoduls informiert. Der Benutzer muss die Information (Fehlermeldung) bestätigen.

INT7 Eine unidirektionale Schnittstelle zwischen dem Sicherheitsmodul und dem Ausgabeverzeichnis. Sie ist unidirektional, da das Sicherheitsmodul gültige Leerungsdatenblöcke (AT+) in das Ausgabeverzeichnis überträgt.

Logische interne Schnittstellen sind die Kanäle über die Daten zwischen räumlich getrennten Teilen des EVG ausgetauscht werden. Alle Teile des EVG sind in der Lage, die Daten bei der Übernahme zu authentifizieren und auf Integrität zu prüfen.

Tabelle 4: Schnittstellen zwischen räumlich getrennten Teilen des Produktes

Komponente 1	Richtung des Datenaustausches	Komponente 2	Beschreibung
ID- Tag Reader	→	EVG- Teil der Fahrzeugsoftware	Der Reader überträgt die identifizierten und gesicherten Daten AT1 zum EVG- Teil der Fahrzeugsoftware. Übertragen wird die gesamte vom ID- Tag gelesene Information.

Komponente 1	Richtung des Datenaustausches	Komponente 2	Beschreibung
			(Daten einschließlich CRC- Prüfsumme) . Physikalisch erfolgt der Datenaustausch über CAN (Controller Area Network [5])
Primärdatenspeicher	→	Transfer- Verzeichnis im Bürorechner	Die gesicherten Leerungsdatenblöcke AT+ stehen in Form einer XML- Datei auf dem Primärdatenspeicher (Memory-Drive) zur Verfügung. Der Primärdatenspeicher wird durch den Benutzer in das Büro getragen und an den Bürorechner angesteckt. Optional können die Daten auch durch eine Luftschnittstelle (z.B. WLAN oder GPRS) zum Bürorechner übertragen werden.
Sekundärdatenspeicher	→	Transfer- Verzeichnis im Bürorechner	Bei einem festgestellten Datenverlust bzw. bei Verfälschung werden die gesicherten Leerungsdatenblöcke AT+ (in Form einer XML- Datei) aus dem Secondary Memory auf einen Memory-Drive kopiert. Der Systemverwalter muss hierfür einen Service- Memory-Drive in den Fahrzeugrechner einlegen. Der Datenspeicher wird durch den Bediener des Fahrzeugrechners in das Büro getragen und an den Bürorechner angesteckt.

Die physischen Kanäle ID- Tag - Fahrzeugsoftware und Fahrzeugsoftware - Sicherheitsmodul sind nicht Bestandteil des Evaluierungsgegenstands. Nur die logischen internen Schnittstellen werden betrachtet.

Weitere Schnittstellen, insbesondere die zu den kommunalen Abrechnungsstellen, sind nicht Bestandteil der Evaluierung. Die Bürosoftware ist auch kein Bestandteil des Evaluierungsgegenstandes.

3 EVG-Sicherheitsumgebung

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.

Der Leerungsdatensatz AT kann optional weitere Datenfelder, wie z.B. Angaben zum Gewicht der Abfälle enthalten.

AT+ Bei der Übertragung der Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro werden die Leerungsdatensätze zu einem Leerungsdatenblock AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in einem WBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem 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 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 einmaligen 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 Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle Leerungsdatenblöcke (At+) von dem Fahrzeugrechner übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer in einem bestimmten Zeitraum durch erneute Anforderung beim Fahrzeugrechner behoben. Dieser Zeitraum ist konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner, der zur Speicherung der Leerungsdatenblöcke (AT+) zur Verfügung steht.

A.Backup Datensicherung

Der Benutzer (S.Trusted) sichert die vom Evaluierungsgegenstand erzeugten Daten regelmäßig im Archiv. Der Evaluierungsgegenstand schützt nicht vor Datenverlusten im Archiv.

A.Installation Korrekte Inbetriebnahme

Es wird sichergestellt, dass die Installation entsprechend des Installationshandbuches durchgeführt wird. Im Handbuch ist beschrieben, wie der EVG korrekt in Betrieb genommen wird.

3.2 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.

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 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.

3.3 Organisatorische Sicherheitspolitik

Die folgende Regel wird für den EVG formuliert:

P.Safe Fehlertoleranz

Die Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Speicherung in einem sekundären Speicher so zu schützen sind, dass die Übertragung der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul nach einem Verlust der Daten in einem primären Speicher möglich ist.

4 Sicherheitsziele

4.1 Sicherheitsziele für den EVG

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.

OT.Inv#1 Erkennung ungültiger Identifikationsdaten

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

OT.Inv#2 Erkennung ungültiger Leerungsdatenblöcke

Der EVG muss jeden Versuch erkennen, willkürliche (im Allgemeinen ungültige) Entleerungsdatenblöcke (AT+) an das Sicherheitsmodul zu übertragen. Der EVG muss Manipulationen der Leerungsdatensätze (AT) während der Bearbeitung und Speicherung innerhalb des Fahrzeugs, sowie Manipulationen der Leerungsdatenblöcke (AT+) durch zufällige Verfälschungen während der Übertragung von der Fahrzeugsoftware zum Sicherheitsmodul erkennen.

OT.Safe Fehlertoleranz

Als Teil des EVG muss die Fahrzeugsoftware 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 möglich ist.

4.2 Sicherheitsziele für die Umgebung

OE.Id ID- Tag

Der ID- Tag ist am Müllbehälter befestigt. Die Identifikationsdaten des Abfallbehälters (AT1) sind im ID- Tag gespeichert. Es werden nur ID- Tags genutzt, deren Identifikationsdaten eindeutig sind. Dies wird dadurch erreicht, dass ausschließlich Read- only- Transponder verwendet werden. Diese werden bereits beim Hersteller mit einer eindeutigen Identifikationsnummer sowie mit einer CRC über die Identifikationsnummer programmiert. Die Identifikationsnummer ist nachträglich nicht mehr änderbar. Mit der CRC wird durch den Empfänger die korrekte Lesung der Identifikationsdaten verifiziert. Die korrekte Zuordnung dieser Daten zur gebührenpflichtigen Person ist durch organisatorische Maßnahmen gewährleistet, die nicht Bestandteil des EVG sind.

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.

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 potentielle Angreifer (S.Attack) innerhalb der IT- Struktur des Büro- PCs muss durch ausreichende Mittel ausgeschlossen werden.

OE.Check **Prüfen der Vollständigkeit**

Es ist sicherzustellen, dass der Nutzer (S.Trusted) in regelmäßigen Intervallen prüft, ob die von der Fahrzeugsoftware zum Büro- PC übertragenen Daten vollständig sind. Bei festgestelltem Datenverlust müssen die Daten durch wiederholte Datenübertragung komplettiert werden. Die Intervalle müssen mit der Datenspeicherkapazität des Fahrzeugcomputers korrespondieren.

OE.Backup **Datensicherung**

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

OE.Installation **Korrekte Inbetriebnahme**

Es ist sicherzustellen, dass die Installation entsprechend des Installationshandbuches durchgeführt wird.

5 IT- Sicherheitsanforderungen

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

Die funktionellen Sicherheitsanforderungen im Kapitel 5.1 sind den Common Criteria Teil 2 [2] entnommen (außer FDP_ITT.5- dies ist in [4] definiert).

Die Anforderungen an die Vertrauenswürdigkeit in Kapitel 5.2 sind den Vertrauenswürdigkeit Komponenten in Common Criteria Teil 3 [3] entnommen.

Kapitel 5.3 identifiziert die IT- Sicherheitsanforderungen denen die IT- Umgebung des EVG entsprechen muss.

Die Sicherheitsanforderungen an die ‚Nicht IT'- Umgebung sind in Kapitel 5.4 beschrieben.

5.1 Funktionale Sicherheitsanforderungen an den EVG

Zuweisungen sind durch **Fettdruck** kenntlich gemacht.

5.1.1 Datenauthentisierung (FDP_DAU)

5.1.1.1 Einfache Datenauthentisierung (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.

FDP_DAU.1.2 Die TSF müssen dem **Benutzer (S.Trusted)** die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten Information bereitstellen.

5.1.2 EVG- interner Transfer (FDP_ITT)

5.1.2.1 Schutz der Integrität des internen Transfers

FDP_ITT.5.1 Die TSF müssen die **Politik zur Datenintegrität** durchsetzen, um Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen materiell getrennten Teilen des TOE (EVG) übertragen werden.

Folgende funktionale Sicherheitspolitik (SFP) Politik der Datenintegrität wird für die Umgebung definiert: „Schutz der Integrität des internen Transfer (FDP_ITT.5)":

Die Nutzerdaten (AT1 und AT+) sollen geschützt werden, um deren Integrität zu wahren.

5.1.3 Integrität der gespeicherten Daten (FDP_SDI)

5.1.3.1 Überwachung der Integrität der gespeicherten Daten (FDP_SDI.1)

FDP_SDI.1.1 Die TSF müssen die innerhalb des TSC gespeicherten Benutzerdaten auf **zufällige Manipulation** bei allen Objekten auf Basis folgender Attribute überwachen:

- **Identifikationsdaten AT1 innerhalb der Identifikationseinheit**
- **Leerungsdatensätze AT während der Speicherung innerhalb des Fahrzeuges**

5.1.4 Fehlertoleranz (FRU_FLT)

5.1.4.1 Verminderte Fehlertoleranz (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**.

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Vertrauenswürdigkeitsstufe: EAL 1

Tabelle 5: Anforderungen für Vertrauenswürdigkeitsstufe EAL1

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ACM	ACM_CAP.1
ADO	ADO_IGS.1
ADV	ADV_FSP.1, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	-
ATE	ATE_IND.1
AVA	-

5.2.1 Konfigurationsmanagement (ACM)

5.2.1.1 Versionsnummern (ACM_CAP.1)

ACM_CAP.1.1D Der Entwickler muss einen Verweisnamen für den TOE (EVG) bereitstellen.

ACM_CAP.1.1C Der Verweisname für den TOE (EVG) muss für jede Version des TOE (EVG) eindeutig sein.

ACM_CAP.1.2C Der TOE (EVG) muss mit seinem Verweisnamen gekennzeichnet sein.

5.2.2 Auslieferung und Betrieb (Delivery and operation) (ADO)

5.2.2.1 Installation, Generierung und Anlauf (Installation, generation, and start-up procedures) (ADO_IGS.1)

ADO_IGS.1.1D Der Entwickler muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Prozeduren dokumentieren.

ADO_IGS.1.1C Die Dokumentation muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Schritte beschreiben.

5.2.3 Entwicklung (Development) (ADV)

5.2.3.1 Informelle funktionale Spezifikation (Informal functional specification) (ADV_FSP.1)

ADV_FSP.1.1D Der Entwickler muss eine funktionale Spezifikation bereitstellen.

ADV_FSP.1.1C Die funktionale Spezifikation muss die TSF und ihre externen Schnittstellen in einem informellen Stil beschreiben.

ADV_FSP.1.2C Die funktionale Spezifikation muss in sich konsistent sein.

ADV_FSP.1.3C Die funktionale Spezifikation muss den Zweck und die Methode des Gebrauchs aller externen TSF-Schnittstellen beschreiben, einschließlich Details der Wirkungen, Ausnahmen und Fehlermeldungen, wie jeweils angemessen.

ADV_FSP.1.4C Die funktionale Spezifikation muss die TSF vollständig darstellen.

5.2.3.2 Informeller Nachweis der Übereinstimmung (Informal correspondence demonstration) (ADV_RCR.1)

ADV_RCR.1.1D Der Entwickler muss eine Analyse der Übereinstimmung aller benachbarten Paare der bereitgestellten TSF-Darstellungen bereitstellen.

ADV_RCR.1.1C Die Analyse muss für jedes Paar benachbarter TSF-Darstellungen nachweisen, dass die gesamte relevante Sicherheitsfunktionalität der abstrakteren TSF Darstellung in der weniger abstrakten TSF-Darstellung korrekt und vollständig verfeinert wurde.

5.2.4 Handbücher (Guidance Documents) (AGD)

5.2.4.1 Systemverwalterhandbuch (Administrator guidance) (AGD_ADM.1)

AGD_ADM.1.1D Der Entwickler muss ein Systemverwalterhandbuch bereitstellen, das an das für Systemverwaltung zuständige Personal gerichtet ist.

AGD_ADM.1.1C Das Systemverwalterhandbuch muss die Systemverwaltungsfunktionen und Schnittstellen beschreiben, die dem Systemverwalter des TOE (EVG) zur Verfügung stehen.

AGD_ADM.1.2C Das Systemverwalterhandbuch muss beschreiben, wie der TOE (EVG) auf sichere Art und Weise zu verwalten ist.

AGD_ADM.1.3C Das Systemverwalterhandbuch muss Warnungen bezüglich Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_ADM.1.4C Das Systemverwalterhandbuch muss alle Annahmen zum Benutzerverhalten beschreiben, die für den sicheren Betrieb des TOE (EVG) relevant sind.

AGD_ADM.1.5C Das Systemverwalterhandbuch muss alle vom Systemverwalter kontrollierten Sicherheitsparameter beschreiben und dabei, wie jeweils angemessen, sichere Werte angeben.

AGD_ADM.1.6C Das Systemverwalterhandbuch muss jede Art von sicherheitsrelevanten Ereignissen bezüglich der auszuführenden Systemverwaltungsfunktionen beschreiben, einschließlich der Änderungen der Sicherheitseigenschaften von Einheiten, die unter Kontrolle der TSF stehen.

AGD_ADM.1.7C Das Systemverwalterhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_ADM.1.8C Das Systemverwalterhandbuch muss alle Sicherheitsanforderungen an die IT- Umgebung beschreiben, die für den Systemverwalter relevant sind.

5.2.4.2 Benutzerhandbuch (User guidance) (AGD_USR.1)

AGD_USR.1.1D Der Entwickler muss ein Benutzerhandbuch bereitstellen.

AGD_USR.1.1C Das Benutzerhandbuch muss die Funktionen und Schnittstellen beschreiben, die den Benutzern des TOE (EVG) zur Verfügung stehen, die nicht für Systemverwaltung zuständig sind.

AGD_USR.1.2C Das Benutzerhandbuch muss den Gebrauch der vom TOE (EVG) bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind, beschreiben.

AGD_USR.1.3C Das Benutzerhandbuch muss Warnungen bezüglich den Benutzern zugänglichen Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_USR.1.4C Das Benutzerhandbuch muss alle Verantwortlichkeiten des Benutzers klar darstellen, die für den sicheren Betrieb des TOE (EVG) notwendig sind, einschließlich derjenigen, die mit den in der Darlegung der EVG-

Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen.

AGD_USR.1.5C Das Benutzerhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_USR.1.6C Das Benutzerhandbuch muss alle Sicherheitsanforderungen an die IT-Umgebung beschreiben, die für den Benutzer relevant sind.

5.2.5 Testen (Tests) (ATE)

5.2.5.1 Unabhängiges Testen – Übereinstimmung (Independent testing conformance) (ATE_IND.1)

ATE_IND.1.1D Der Entwickler muss den TOE (EVG) zum Testen bereitstellen.

ATE_IND.1.1C Der TOE (EVG) muss sich zum Testen eignen.

5.3 Sicherheitsanforderungen an die IT- Umgebung

Es gibt keine speziellen Sicherheitsanforderungen an die IT- Umgebung.

5.4 Sicherheitsanforderungen an die nicht IT- Umgebung

R.Id **Identification unit (ID- Tag)**

Der Benutzer muss folgendes absichern:

Der ID- Tag ist am durch die Identifikationsdaten zu identifizierenden Müllbehälter 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.

R.Trusted **Vertrauenswürdiges Personal**

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

R.Access **Zugangsschutz**

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.

R.Check **Prüfung der Vollständigkeit**

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.

R.Backup **Datensicherung**

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

R.Installation **Korrekte Inbetriebnahme**

Die Installation muss entsprechend des Installationshandbuches durchgeführt werden.

6 EVG-Übersichtsspezifikation

6.1 EVG-Sicherheitsfunktionen

6.1.1 TSF_Crc_ccittv

TSF_Crc_ccittv prüft die AT1, indem die CRC über die vom ID- Tag empfangenen Daten AT1 berechnet und mit der ebenfalls empfangenen CRC- Checksumme verglichen wird. Beim Übereinstimmen von berechneter und empfangener CRC- Checksumme wird AT1 zurückgeliefert, ansonsten nicht.

6.1.2 TSF_GenerateAT_Check

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

Es wird eine CRC32- Checksumme berechnet, bei der Bildung werden der AT sowie die Fahrzeugkennung einbezogen.

Die Fahrzeugkennung und die CRC32- Checksumme werden an den Aufrufer zurückgegeben und müssen 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.

6.1.3 TSF_GenerateATPlus_Check

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

Es wird eine CRC32- Checksumme berechnet, bei der Bildung werden der AT+ sowie die Fahrzeugkennung einbezogen.

Die Fahrzeugkennung und die CRC32- Checksumme werden an den Aufrufer zurückgegeben und müssen 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.

6.1.4 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 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.

6.1.5 TSF_Check_ATPlus

Die Funktion berechnet eine CRC32- Checksumme, bei der Bildung werden der an das Sicherheitsmodul übergebene Leerungsdatenblock AT+ sowie die ebenfalls übergebene Fahrzeugkennung einbezogen.

Die berechnete CRC32- Checksumme wird mit der mit dem AT+ an das Sicherheitsmodul übergebenen CRC32- Checksumme verglichen

Es wird geprüft, ob eine gültige Fahrzeugkennung mit dem Leerungsdatenblock AT+ übergeben wurde.

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 korrekte Weiterverarbeitung genutzt.

6.1.6 TSF_Check_AT

Die Funktion berechnet eine CRC32- Checksumme, bei der Bildung werden der an das Sicherheitsmodul übergebene Leerungsdatensatz AT sowie die ebenfalls übergebene Fahrzeugkennung einbezogen.

Die berechnete CRC32- Checksumme wird mit der mit dem AT und der Fahrzeugkennung an das Sicherheitsmodul übergebenen CRC32- Checksumme verglichen.

Es wird geprüft, ob eine gültige Fahrzeugkennung mit AT übergeben wurde.

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 korrekte Weiterverarbeitung genutzt.

6.2 Maßnahmen zur Vertrauenswürdigkeit

Tabelle 6: Vertrauenswürdigkeitskomponenten und Maßnahmen

Komponente	Maßnahme
ACM_CAP.1	Jede SW- Komponente besitzt eine Versionsnummer, die durch den Nutzer abgefragt werden kann Die Transponder besitzen eine eindeutige Typbezeichnung. Durch den Hersteller wird die eindeutige Seriennummer gewährleistet.
ADO_IGS.1	Das System wird in einem konfigurierten und getesteten Zustand ausgeliefert. Die MOBA- interne Qualitätskontrolle schreibt vor, wie der Auslieferungszustand zu prüfen ist, welche Testschritte zu unternehmen sind und in welcher Form dies zu protokollieren ist.
ADV_FSP.1	MAWIS_Rev3_ADV_FSP enthält die Beschreibung der für den Benutzer sichtbaren Schnittstellen der EVG-Sicherheitsfunktionen und des Verhaltens dieser EVG-Sicherheitsfunktionen.
ADV_RCR.1	MAWIS_Rev3_ADV_RCR.doc stellt für jedes Paar benachbarter Darstellungen von EVG-Sicherheitsfunktionen dar, dass die gesamte relevante Sicher-

Komponente	Maßnahme
	heitsfunktionalität der abstrakteren TSF Darstellung in der weniger abstrakten TSF-Darstellung korrekt und vollständig verfeinert wurde.
AGD_ADM.1	Das Systemverwalterhandbuch dokumentiert, wie der korrekte Betrieb von MAWIS zu prüfen und wie im Fehlerfall zu reagieren ist. Insbesondere beschreibt er, wie Daten aus dem sekundären Datenspeicher des Fahrzeugrechners erneut an den Bürorechner zu übertragen sind.
AGD_USR.1	Das Benutzerhandbuch stellt alle Informationen zur Verfügung, die der Benutzer zum sicheren Betrieb des EVG benötigt.
ATE_IND.1	Es wird ein zum Testen geeigneter EVG zur Verfügung gestellt.

7 PP-Postulat

Der EVG stimmt mit den Anforderungen des Schutzprofils „Waste Bin Identification Systems WBIS-PP“, Version 1.04 überein.

Die Sicherheitsziele für den EVG, die funktionalen Sicherheitsanforderungen an den EVG und die Anforderungen an die Vertrauenswürdigkeit des EVG wurden aus dem Schutzprofil [4] übernommen.

Folgende Verfeinerungen und Ergänzungen wurden vorgenommen:

Die Annahmen für die EVG-Sicherheitsumgebung wurden um A.Installation erweitert (Korrekte Inbetriebnahme).

Bei den Sicherheitszielen für die Umgebung wurde OE.Id verfeinert.

Die Sicherheitsziele für die Umgebung wurden um OE.Installation erweitert (Korrekte Inbetriebnahme).

Die Sicherheitsanforderungen an die nicht IT- Umgebung wurden um R.Installation erweitert (Korrekte Inbetriebnahme).

8 Erklärungen

8.1 Einführung

Die Tabellen in den Abschnitten 8.2.1 und 8.2.2 stellen die Verknüpfung von Sicherheitszielen und Sicherheitsanforderungen an den EVG dar.

8.2 Erklärung der Sicherheitsziele

8.2.1 Abdeckung der Sicherheitsziele

Tabelle 7: Übersicht Sicherheitsziele

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

8.2.2 Zulänglichkeit der Sicherheitsziele

8.2.2.1 Zulänglichkeit der Politiken und der Sicherheitsziele

P.Safe (Fehlertoleranz) ist die Verfügbarkeit der Leerungsdatenblöcke (AT+), auch im Falle, dass die Leerungsdatenblöcke im Primärdatenspeicher der Fahrzeugsoftware verloren gegangen sind. Dies wird durchgesetzt, indem die Daten zusätzlich in einem sekundären Datenspeicher gehalten werden. Dies ist exakt im Sicherheitsziel OT.Safe wiederholt, so dass dieses Ziel ausreichend für P.Safe ist.

8.2.2.2 Zulänglichkeit der Bedrohungen und der Sicherheitsziele

T.Man (Manipulierte Identifikationsdaten) behandelt Angriffe, durch die Identifikationsdaten (AT1) im ID- Tag verfälscht werden. Gemäß OT.Inv#1 werden verfälschte Identifikationsdaten (AT1) vom EVG erkannt (nachdem sie durch den Reader gelesen wurden). Das wirkt der Bedrohung T.Man direkt entgegen.

T.Jam#1 (Störung der Identifikationsdaten) behandelt Angriffe, in denen gestörte Identifikationsdaten an den Reader übergeben werden. Gemäß OT.Inv#1 werden verfälschte Identifikationsdaten (AT1) vom EVG erkannt (nachdem sie durch den Reader gelesen wurden). Das wirkt der Bedrohung T.Jam#1 direkt entgegen.

T.Create (Ungültige Leerungsdatensätze) behandelt Angriffe, in denen willkürlich Leerungsdatensätze erstellt und dann an das Sicherheitsmodul übergeben werden. Gemäß OT.Inv#2 wird jeder Versuch erkannt, willkürliche Leerungsdatenblöcke (z.B. ungültige) an das Sicherheitsmodul zu übergeben. Das wirkt der Bedrohung T.Create direkt entgegen.

T.Jam#2 (Verfälschte Leerungsdatensätze) richtet sich gegen Angriffe, in denen Leerungsdatensätze (AT) während der Verarbeitung und Speicherung auf dem Fahrzeug verfälscht werden oder in 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.

8.2.2.3 Zulänglichkeit der Annahmen und der Sicherheitsziele

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 ausreichend für A.Id.

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

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 ausreichend für A. Access.

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 ausreichend für A.Check.

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 ausreichend für A.Backup.

A.Installation (Korrekte Inbetriebnahme) sichert, dass der EVG entsprechend der Dokumentation in Betrieb genommen wird. Es sichert auch, dass im Handbuch steht, wie der EVG korrekt in Betrieb genommen wird. Da das Ziel OE.Installation festlegt, dass der EVG entsprechend des Handbuches in Betrieb genommen werden muss, ist es ausreichend für A.Installation.

8.3 Erklärung der Sicherheitsanforderungen

8.3.1 Abdeckung der Sicherheitsanforderungen

Tabelle 8: Zuordnung der funktionellen Sicherheitsanforderungen zu den Sicherheitszielen des EVG

Sicherheitsziele / Funktionelle 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**

Tabelle 9: Zuordnung der Sicherheitsanforderung an die Umgebung zu den Sicherheitszielen der Umgebung

EVG- Sicherheitsziele / Sicherheits-anforderungen an die Umgebung	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.Installation
R.Id	**X**					
R.Trusted		**X**				
R.Access			**X**			
R.Check				**X**		
R.Backup					**X**	
R.Installation						**X**

8.3.2 Zulänglichkeit der Sicherheitsanforderungen

8.3.2.1 Zulänglichkeit der EVG- Sicherheitsanforderungen und gegenseitige Unterstützung

OT.Inv#1 (Erkennung gestörter Identifikationsdaten) zielt auf die Erkennung der Manipulation von Identifikationsdaten (AT1) der Leerungsdatensätze (AT) innerhalb des ID- Tag und während der Übertragung zwischen ID- Tag und Fahrzeugsoftware, welche verschiedene 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 physikalisch 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. Diese stellen physikalisch von einander getrennte Teile des EVG dar. Der Schutz der Anwenderdaten AT+, um ihre Integrität zu sichern, ist in FDP_ITT.5 für die Übertragung von Daten zwischen physikalisch voneinander getrennten Teilen des EVG gefordert. Die Integrität der Daten zu sichern, schützt direkt gegen Manipulation der Daten. OT.Inv#2 zielt auch auf die Erkennung ungültiger Leerungsdatensätze (AT) während der Verarbeitung und Speicherung im Fahrzeug und auf Manipulationen von Leerungsdatenböcken (AT+), die zum Sicherheitsmodul übertragen werden. Der EVG hat gemäß FDP_DAU.1 die Fähigkeit, Nachweise zu erzeugen und ermöglicht es so dem Nutzer, die Gültigkeit der Daten zu überprüfen. Der Schutz der Integrität der im Fahrzeug gespeicherten Anwenderdaten (AT) wird durch FDP_SDI.1 gefordert und begegnet direkt der zufälligen Manipulation dieser Daten. Die Forderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig für die Authentizität und Integrität der Daten. 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+) von der Fahrzeugsoftware zum Sicherheitsmodul relevanten Daten auch für den Fall eines Datenverlustes im primären Datenspeicher der Fahrzeugsoftware. Die Durchführung dieses Datentransfers mit Hilfe eines zweiten Datenspeichers nach dem Verlust der Daten im Primärdatenspeicher wird durch den EVG gemäß FRU_FLT.1 realisiert.

8.3.2.2 Zulänglichkeit der Sicherheitsanforderungen an die Umgebung des EVG

OE.Id (Identifikationseinheit) wird durch R.Id zur Verfügung gestellt, da R.Id fordert, was durch das Ziel OE.Id festgelegt wird.

OE.Trusted (Vertrauenswürdiges Personal) wird durch R.Trusted zur Verfügung gestellt, da R.Trusted fordert, was durch das Ziel OE.Trusted festgelegt wird.

OE.Access (Zugangsschutz) wird durch R.Access zur Verfügung gestellt, da R.Access fordert, was durch das Ziel OE.Access festgelegt wird.

OE.Check (Prüfung der Vollständigkeit) wird durch R.Check zur Verfügung gestellt, da R.Check fordert, was durch das Ziel OE.Check festgelegt wird.

OE.Backup (Datensicherung) wird durch R.Backup zur Verfügung gestellt, da R.Backup fordert, was durch das Ziel OE.Backup festgelegt wird.

OE.Installation (Korrekte Inbetriebnahme) wird durch R.Installation zur Verfügung gestellt, da R.Installation fordert, was durch das Ziel OE.Installation festgelegt wird.

8.4 Ausdrücklich festgelegte Sicherheitsanforderungen

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 von einander 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 es nur auf die Manipulation von Daten zielt.

8.5 Erklärung der EVG-Übersichtsspezifikation

8.5.1 Zusammenwirken der Sicherheitsfunktionen

Tabelle 10: Gegenüberstellung funktioneller Sicherheitsanforderungen und Sicherheitsfunktionen des EVG

Sicherheitsfunktion / Funktionelle Sicherheitsanforderungen	TSF_Crc_ccittv	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_Crc_ccittv 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_Crc_ccittv 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.

8.6 Erklärung zur Anforderung an die Vertrauenswürdigkeit des EVG

Die Vertrauenswürdigkeitsstufe für den EVG ist EAL1. Diese Vertrauenswürdigkeitsstufe bietet gegenüber einem nicht evaluierten IT- Produkt oder -System einen bedeutenden Zuwachs an Sicherheit, indem es Vertrauen in die korrekte Funktion schafft. Dabei werden die angenomme-

nen Bedrohungen als gering betrachtet. Außerdem werden durch die Gegenmaßnahmen des EVG eher geringe Werte geschützt.

Deshalb bietet EAL1 angemessenen Schutz.

8.7 Erklärung der Maßnahmen zur Vertrauenswürdigkeit

Kapitel 6.2 erläutert, welche Maßnahmen zur Vertrauenswürdigkeit der EVG ergreift. Damit wird den Forderungen des Schutzprofils [4] entsprochen.

8.8 Erklärung zur Stärke der Sicherheitsfunktionen des EVG

Das Schutzprofil [4] enthält in den Anforderungen an die Vertrauenswürdigkeit keine Forderungen zur Stärke der Sicherheitsfunktionen des EVG. Aus diesem Grund wird keine Stärke der Sicherheitsfunktionen des EVG angegeben.

8.9 Erklärung zur gegenseitigen Unterstützung der funktionalen Anforderungen

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

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 11: Abhängigkeiten der funktionalen Anforderungen

Anforderung	Abhängigkeiten	Erfüllt
FDP_DAU.1	keine	Ja
FDP_ITT.5	keine	Ja
FDP_SDI.1	keine	Ja
FRU_FLT.1	FPT_FLS.1	Siehe 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.

8.10 Erklärung zu den PP- Postulaten

Der EVG erfüllt alle Anforderungen des Schutzprofils [4].

9 Quellen

[1] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model
August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements
August 2005, Version 2.3

[3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements
August 2005, Version 2.3.

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

[5] CAN Specification
Version 2.0
1991, Robert Bosch GmbH, Postfach 30 02 40, D-70442 Stuttgart
www.semiconductors.bosch.de/pdf/can2spec.pdf

10 Anhang 1: Transponder Übersicht

Dieser Anhang erläutert die technischen Kernparameter sowie die Bezeichnungen der Transpondertypen, die zur Herstellung des Identifikationssystems MAWIS Rev. 3.0 zugelassen sind.

Es werden Transponder eingesetzt, deren Datenübertragung der im ISO 11785 beschriebenen entspricht.

ISO 11785 beschreibt das Abfrageprotokoll für Full-Duplex (FDX) und Half-Duplex (HDX) Transponder. In diesem Protokoll werden unter anderem die Transponder ID (AT1) und eine 16 Bit Prüfsumme nach CCITT-CRC übertragen.

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

Die Transponder verfügen mindestens über eine feste 32/40/64 Bit Unique ID/OEM-Nummer.

Alle MOBA Transponder, mit den folgenden Artikelnummern entsprechen diesen Parametern und sind zur Herstellung des Identifikationssystems MAWIS Rev. 3.0 zugelassen:

MOBA- Artikel- Nummern: 02-21-00000 bis 02-21-02000