Sicherheitsvorgaben für das c-trace Abfallbehälter-Identifikations-System c-ident

Inhaltsverzeichnis

Dies sind die Sicherheitsvorgaben (Security Target – ST) für die Evaluierung und Zertifizierung des c-trace Abfall-Behälter-Identifikations-Systems c-ident nach den Common Criteria (CC) for IT Security Evaluation und auf der Grundlage des Schutzprofils „Protection Profile – Waste Bin Identification Systems (WBIS-PP), Version 1.04".

Alle Passagen in blauer Schriftfarbe sind dem WBIS-PP entnommen oder sind eine direkte Übersetzung dessen Inhalts.

1 ST-Einführung

1.1 ST-Verweis

ST Titel	Sicherheitsvorgaben für das c-trace Abfall-Behälter-Identifikations-System c-ident
ST Version	1.14
ST Datum	09.03.2020
ST Verfasser	Ralf Bortfeldt, c-trace GmbH Thomas Kemner, c-trace GmbH Roland Vogt, DFKI GmbH (redaktionelle und strukturelle Bearbeitung)

1.2 EVG-Verweis

EVG Name	c-secure ident
EVG Version	2.0

1.3 Übersicht von EVG und Gesamtsystem

Ziel dieser Sicherheitsvorgaben ist es, funktionale Anforderungen und Vertrauenswürdigkeitsanforderungen für die EVG-Komponenten (Evaluierungsgegenstand – EVG) c-secure ident des c-trace Abfall-Behälter-Identifikations-System (Waste Bin Identification System – WBIS) c-ident zu spezifizieren. Die Sicherheitsvorgaben definieren die Sicherheitsanforderungen der EVG-Teile für die Übertragung und Speicherung der aufgezeichneten Leerungsdaten. Der EVG ist klar vom Gesamtsystem c-ident abgegrenzt, welches keine zusätzlichen Funktionen und Sicherheitsanforderungen umsetzt.

1.3.1 Eigenschaften des Abfall-Behälter-Identifikations-Systems c-ident

Abfall-Behälter-Identifikations-Systeme (Waste Bin Identification Systems – WBIS) im Sinne dieses Dokuments sind Systeme, durch die 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 diesen Systemen nicht um die direkte Identifikation von Abfällen, sondern um die Identifikation der Behälter, in denen Abfälle zur Entsorgung bereitgestellt werden.

Das c-trace Abfall-Behälter-Identifikations-System c-ident erfasst Abfallbehälter mit Hilfe der RFID-Technologie automatisch und zuverlässig. Die Abfallbehälter werden mit einem ID-Tag zur eindeutigen Zuordnung zum Eigentümer ausgerüstet. Hierzu stehen verschiedene Chiptypen (Transponder) in diversen Bauformen für die unterschiedlichsten Einsatzzwecke zur Verfügung.

Das c-trace Abfall-Behälter-Identifikations-System c-ident wird im Bereich der Abfallentsorgung eingesetzt, wo Abrechnungssysteme gefordert werden, die eine verursacher- und mengengerechte Gebührenabrechnung ermöglichen. 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. 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.

Ziel ist nicht nur, eine verursachergerechte Gebührenveranlagung gemäß einer vorgegebenen Satzung zu realisieren. Das c-trace Abfall-Behälter-Identifikations-System c-ident soll vielmehr die Basis sein, Abläufe transparent zu gestalten und zu optimieren. Neben dem reinen Behältermanagement ist die Bereitstellung sinnvoll auswertbarer Informationen in zunehmendem Maße ein wichtiges Anliegen.

Den Städten und Gemeinden bietet die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) die notwendige Sicherheit insbesondere beim gebührenrelevanten Einsatz des c-trace Abfall-Behälter-Identifikations-Systems c-ident. Die Zertifizierung von c-secure ident gemäß Schutzprofil „Protection Profile – „Waste Bin Identification Systems (WBIS-PP)" hat auch deshalb eine besondere Bedeutung für die Städte und Gemeinden, da das Anforderungsprofil gemeinsam mit ihrer Dachorganisation, dem Städte- und Gemeindebund festgelegt wurde.

Abfall-Behälter-Identifikations-Systeme (Waste Bin Identification Systems – 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. Im c-trace Abfall-Behälter-Identifikations-System c-ident sind daher die für die Abrechnung relevanten Daten (Behälteridentifikation, Zeitstempel, Leerungsdaten, Fahrzeugidentifikation, Ereigniszählerstand) vor Manipulation und Verlust geschützt. Für die Gewährleistung der technischen Funktionsfähigkeit genügt ein geeigneter Schutz vor Manipulation durch rein zufällige Verfälschung.

Alle für die Abrechnung relevanten Daten werden bei der Leerung eines Abfallbehälters an einem Sammelfahrzeug automatisch erfasst. Das System ist so aufgebaut, dass es völlig unabhängig von anderen Teilen des Fahrzeugs nur auf der Schüttung installiert werden kann. Selbst bei Fahrzeugausfall (z.B. Getriebeschaden) kann die Schüttung an einem anderen Fahrzeug angebaut und das System weiterbetrieben werden. Optional ist eine Installation von Teilen des Systems (insb. Fahrzeugrechner) im Fahrerhaus möglich.

Das c-trace Abfall-Behälter-Identifikations-System c-ident bietet Schutz vor Datenverlust und rein zufälliger Datenverfälschung bis in die Bürosoftware. Der EVG c-secure ident gewährleistet mit seiner Sicherheitsfunktionalität die Gültigkeit, Integrität und Vollständigkeit der zu schützenden Daten. Das c-trace Abfall-Behälter-Identifikations-System c-ident gewährleistet jedoch nicht die Vertraulichkeit der Daten, insb. beinhaltet es keine Funktionalität zur Verschlüsselung.

1.3.2 Verwendung und wesentliche Sicherheitsmerkmale von c-secure ident

Am Fahrzeug werden die Abfallbehälter eindeutig und sicher identifiziert und optional auch gewogen. Ausgehend von der aus dem ID-Tag (Teil des EVG) gelesenen Identifikationsnummer des Behälters wird ein Leerungsdatensatz gebildet. Dazu prüft die Sicherheitsbibliothek c-secure vehicle (Teil des EVG) die vom Transponder eingelesenen Daten des am Abfallbehälter angebrachten Chips auf Integrität, ergänzt korrekt eingelesene Daten um Datum und Uhrzeit der Leerung, zusätzliche Leerungsdaten, die Fahrzeugidentifikation als Gültigkeitsmerkmal und den Ereigniszählerstand und fügt ein Integritätsmerkmal an.

Die Sicherheitsbibliothek c-secure vehicle (Teil des EVG) fasst die so gebildeten Leerungsdatensätze zu einem Leerungsdatenblock zusammen, fügt zusätzlich ein Integritätsmerkmal hinzu und speichert jeden Leerungsdatenblock zusammen mit der Fahrzeugidentifikation als Gültigkeitsmerkmal dann redundant auf zwei getrennten Speichermedien im Fahrzeugrechner, damit diese auch bei einem Datenverlust im ersten Speichermedium wiederhergestellt werden können.

Nach Abschluss oder während einer Leerungstour des Fahrzeuges werden alle gesammelten Daten von der Fahrzeugsoftware außerhalb des EVG an einen zentralen Server drahtlos übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Von hier aus können diese Daten regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

Dazu werden die Leerungsdatenblöcke an das Sicherheitsmodul c-secure office (Teil des EVG) im Bürorechner (Server) übertragen. Dieses Sicherheitsmodul prüft die empfangenen Leerungsdatenblöcke und -sätze auf Gültigkeit und Integrität und kennzeichnet sie mit dem Prüfergebnis. Nach erfolgreicher Prüfung durch das Sicherheitsmodul werden die Leerungsdatenblöcke und -sätze im zentralen Datenbestand zur weiteren Verarbeitung durch die Bürosoftware bereitgestellt.

1.4 Beschreibung des Gesamtsystems c-ident

In diesem Abschnitt werden der Kontext des Gesamtsystems c-ident mitsamt den EVG-Teilen beschrieben. Dieses Vorgehen ist notwendig um ein generelles Verständnis über den Zweck und die Funktionsweise der EVG-Teile zu ermöglichen. Eine Betrachtung der dedizierten Sicherheitsfunktionen des EVG findet in Abschnitt 1.5 statt.

Das c-trace Abfall-Behälter-Identifikations-System c-ident besteht aus folgenden Komponenten:

- ID-Tag mit den Identifikationsdaten des Abfallbehälters.
- Abfallsammelfahrzeug mit dem (ID-Tag-) Reader, Fahrzeugrechner und einem optionalem Wiege-, Volumenmess- oder ähnlichem System.
  Die Fahrzeugsoftware mit der Sicherheitsbibliothek c-secure vehicle ist auf dem Fahrzeugrechner installiert.
- Zentraler Server
  Die Serverkomponenten der Bürosoftware mit dem Sicherheitsmodul c-secure office sind auf einem zentralen Server in der c-trace Geschäftsstelle oder optional auf einem zentralen Server in der Geschäftsstelle des Endanwenders installiert.
- Bürorechner im Büro des Endanwenders.
  Die Clientkomponenten der Bürosoftware sind auf dem Bürorechner des Endanwenders installiert.

Fahrzeug, zentraler Server, und Bürorechner des Endanwenders sind ausschließlich vertrauenswürdigen Personen zugänglich.

Die folgende Abbildung 1 gibt einen Überblick über das c-trace Abfall-Behälter-Identifikations-System c-ident. Die verschiedenen Schnittstellen werden durch Pfeile dargestellt. Die Komponenten des EVG *c-secure ident* sind in der Abbildung durch grüngefüllte Kästchen gekennzeichnet. Weitere Angaben zu den Komponenten des EVG *c-secure ident* sind in Tabelle 4 aufgeführt.

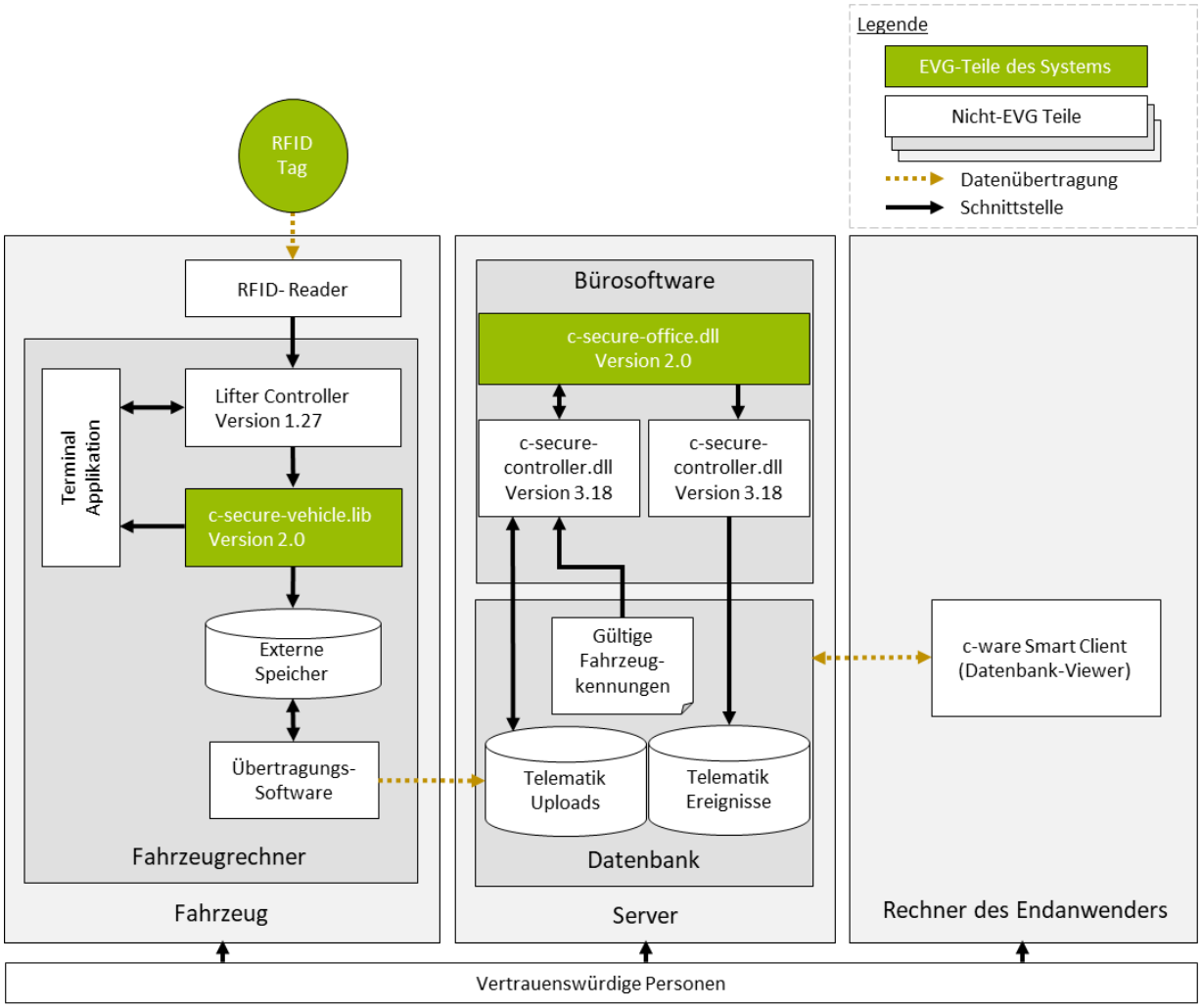


Abbildung 1: c-trace Abfall-Behälter-Identifikations-System c-ident

Alle Transpondertypen gemäß Anhang „Transponder Übersicht" sind Teil des EVG.

Der Fahrzeugrechner beinhaltet die Fahrzeugsoftware und zwei externe Speicher. Die Fahrzeugsoftware besteht aus der Sicherheitsbibliothek c-secure vehicle und aus weiteren Komponenten, die zusammenfassend mit c-ident vehicle bezeichnet werden. Nur die Sicherheitsbibliothek c-secure vehicle ist Teil des EVG. Die externen Speicher (Speichermodule) gehören ebenfalls nicht zum EVG. Ein Speichermodul wird als Primärspeicher und das andere als Sekundärspeicher eingesetzt.

Der zentrale Server beinhaltet die Serverkomponenten der Bürosoftware sowie eine Datenbank zum Empfang der Leerungsdatenblöcke (Telematik-Uploads genannt) und zur Bereitstellung der geprüften Leerungsdatenblöcke und -sätze (Telematik-Ereignisse genannt). Die Serverkomponenten der Bürosoftware bestehen aus dem eigenständigen Sicherheitsmodul c-secure office und aus weiteren Komponenten, die zusammenfassend als c-ware office bezeichnet werden. Nur das Sicherheitsmodul c-secure office ist Teil des EVG. Über zwei Verarbeitungspfade steuert c-secure-controller den Zugriff zwischen der Datenbank und dem Sicherheitsmodul c-secure office, welches für die Gültigkeitsprüfung zudem eine Liste der gültigen Fahrzeugkennungen erhält.

Über die Clientkomponente der Bürosoftware mit grafischer Benutzerschnittstelle (c-ware smart client) kann der Endanwender die Datenbank auslesen bzw. die gültigen Fahrzeugkennungen einstellen. Die Clientkomponente der Bürosoftware ist nicht Teil des EVG.

Das c-trace Abfall-Behälter-Identifikations-System c-ident 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.

Die Abfallbehälter werden mit einem Datenträger (RFID Tag) ausgestattet. Das RFID Tag speichert Identifikationsdaten, die zur Identifikation des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifikationsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Leser außerhalb des EVG ausgelesen. Die Identifikationsdaten werden dann an die Fahrzeugsoftware weitergeleitet. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen durch rein zufällige Verfälschungen werden von der Sicherheitsbibliothek c-secure vehicle erkannt. Optional werden zusätzliche Leerungsdaten wie das Gewicht der Abfälle oder der Füllstand der Tonne durch eine entsprechende Sensorik im Fahrzeug ermittelt und parallel zu den Identifikationsdaten an die Fahrzeugsoftware übermittelt. Die Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware ergänzt diese Daten um Datum- und Zeitangaben, die außerhalb des EVG ermittelt werden, fügt die Fahrzeugidentifikation als Gültigkeitsmerkmal, den Ereigniszählerstand sowie ein Integritätsmerkmal hinzu und bildet daraus ein Telematik-Ereignis (Leerungsdatensatz). Ein oder mehrere Telematik-Ereignisse werden von der Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware zu einem Telematik-Upload (Leerungsdatenblock) zusammengefasst, dem zusätzlich ein Integritätsmerkmal hinzugefügt wird. Die Fahrzeugidentifikation als Gültigkeitsmerkmal ist im Dateinamen des Telematik-Uploads abgebildet. Der Dateiname selbst liegt außerhalb des Leerungsdatenblocks und wird über das Integritätsmerkmal nicht abgesichert.

Die Telematik-Uploads werden über das Sicherheitsmodul c-secure office an die Bürosoftware übermittelt. Die Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware sorgt durch redundante Speicherung in zwei externen Speichermedien dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist. Bei der Übermittlung der Telematik-Uploads an die Bürosoftware wird durch das Sicherheitsmodul c-secure office sichergestellt, dass nur die in einem registrierten Fahrzeugrechner erstellten Datenblöcke als gültig anerkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt. Dazu werden die auf den Server übertragenen Telematik-Uploads vom Verarbeitungsmodul außerhalb des EVG, gemeinsam mit den gültigen Fahrzeugkennungen in das Sicherheitsmodul c-secure office eingereicht und nach der ausschließlich dort stattfindenden Prüfung wieder vom Verarbeitungsmodul mitsamt Prüfergebnis gespeichert. Auch die aus einem gültigen Telematik-Upload extrahierten Telematik-Ereignisse werden geprüft und mit ihrem Prüfergebnis gespeichert.

Die Clientkomponente kann lesend auf geprüfte und ungeprüfte Telematik-Uploads und auf geprüfte Telematik-Ereignisse zugreifen sowie Fahrzeugkennungen konfigurieren (Fahrzeugidentifikationen auf gültig oder ungültig stellen). Die Telematik-Uploads können als Textdatei von der

Clientkomponente der Bürosoftware auf den Rechner des Endanwenders exportiert werden. Sie können optional ausgewertet werden, um z.B. weitere denkbare Angriffe (ungültige, kopierte Identifikationsdaten usw.) abzuwehren. Die Telematik-Ereignisse, die in den Telematik-Uploads enthalten sind, oder die Telematik-Uploads selbst werden an externe Systeme (z.B. bei den Kommunen) zur Abrechnung mit dem Kunden weitergeleitet. Solche externen Systeme können neben der Abrechnungs- auch andere Funktionalität (z.B. das Erkennen von möglichem Missbrauch durch wiedereingespielte Telematik-Uploads usw.), die die Sicherheitsfunktionalität des Evaluierungsgegenstands c-secure ident ergänzen, bereitstellen.

Das ID-Tag und die Datenübertragungsstrecke zwischen dem ID-Tag und der Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware, die im Fahrzeug gespeicherten Daten sowie die Übertragungsstrecke zwischen der Fahrzeugsoftware und dem Sicherheitsmodul c-secure office sind potenziellen Angriffen ausgesetzt. Bei der Betrachtung des Angriffspotentials 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 (Server und Umgebung des Endanwenders) realisiert.

Notwendige Nicht-EVG-Bestandteile (Hardware/Software/Firmware)

In diesem Abschnitt wird eine Auflistung der für den Betrieb der softwaretechnischen EVG-Teile benötigten Hardware, Firmware und Software aufgeführt. Die nachfolgenden Unterpunkte orientieren sich an den beiden definierten Software-Komponenten des EVG (vgl. Tabelle 4).

c-secure-vehicle

Das Fahrzeugsystem besteht aus mindestens drei Komponenten. Der RFID-Reader, der über die Anschaltbox mit dem Fahrzeugrechner verbunden ist. Eine Anschaltbox, in der die GPS-Maus, das UMTS-Modem und die Speichermedien untergebracht sind, und der Fahrzeugrechner selbst. Optional kann noch ein Wiegesystem eingebunden werden.

Nr.	Hardware	Anforderungen
1	RFID-Reader	- gemäß DIN 30745 - CAN-Schnittstelle
2	Fahrzeugrechner	- Embedded Linux - 32bit Prozessor; ARM11; i.MX35 - RS232, USB und CAN- Schnittstelle - Lifter Controller V1.27 - Terminal Applikation (qtTerm2) - Übertragungssoftware (qtTransferDaemon)
3	Anschaltbox für Fahrzeugrechner	- TCU-Box; Art.Nr. 100935 - GPS-Maus; Protokoll NMEA 0183 - UMTS-Modem; GL8200 - 2GB USB-Sticks; Dateisystem ext3
4	Wiegesystem (optional)	- CAN-Schnittstelle

Tabelle 1: Physical Scope des Fahrzeugsystems

c-secure-office

Die Bürosoftware erstreckt sich als verteilte Anwendung auf die Serverumgebung sowie auf den PC des Endanwenders. Web- und Datenbankserver werden in der nachfolgenden Auflistung auf einer Maschine ausgewiesen. Eine Aufteilung der beiden Server auf zwei virtuelle oder physische Maschinen ist optional möglich. Insbesondere die Hardwareausstattung, die Betriebssysteme und die Versionen der Dienste und Laufzeitumgebungen sind als Mindestanforderungen aufzufassen. Die Bibliotheken c-secure office und c-secure controller sind als DLL-Dateien Bestandteil der serverseitigen Bürosoftware auf dem Webserver der Serverumgebung. c-secure controller bleibt in der Version 3.18 fixiert.

Nr.	Hardware/ Betriebssystem	Laufzeitumgebungen/Dienste/Software
1	VDSL-Anschluss inkl. Firewall	*nicht definiert*
2	Webserver und Datenbankserver: Windows Server ab 2012 R2 mit folgender Ausstattung: - 4-8 CPU-Kerne - 6-16 GB RAM - 200 GB HDD	- .NET-Framework 4.7.1 (deutsches Sprachpaket) - IIS Version 7 - Microsoft SQL Server ab 2012 inkl. Kundendatenbank - Serverteil der Bürosoftware inkl. Sicherheitsmodul c-secure office (EVG-Teil) - c-secure controller V3.18

Tabelle 2: Physical Scope der Serverumgebung

Nr.	Hardware/ Betriebssystem	Laufzeitumgebungen/Dienste/Software
1	VDSL-Anschluss inkl. Firewall	*nicht definiert*
2	Endanwender-PC: Microsoft Windows 7 32bit mit folgender Ausstattung: - 4 GB RAM - 4 GB HDD - 2,5 GHz CPU - Direct X 11 fähige Grafikkarte - Monitor mit einer Auflösung von 1280x1024 Pixel	- .NET-Framework 4.7.1 (deutsches Sprachpaket) - c-ware Smart Client - Ein Gängiges Zip-Archivprogramm (z.B. 7-Zip Version 16.4)

Tabelle 3: Physical Scope der Anwenderumgebung

1.5 Beschreibung des EVG c-secure-ident

Der Evaluierungsgegenstand besteht aus dem ID-Tag, der Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware, dem Sicherheitsmodul c-secure office der Bürosoftware und der Benutzerdokumentation (s. Tabelle 5). Alle anderen Komponenten (siehe auch Abbildung 1) sind nicht Bestandteil des Evaluierungsgegenstands und gehören zu dessen Umgebung. Auch die übrigen Komponenten der Fahrzeugsoftware (c-ident vehicle) und der Bürosoftware (c-ware office und c-ware Smart Client) sind auch keine Bestandteile des Evaluierungsgegenstandes.

Nr.	Typ	Bezeichnung	Version	Anmerkung
1	HW	ID-Tags (Chips / Transponder)	Siehe Anhang „Transponder Übersicht"	Bei den ID-Tags handelt es sich um passive Chips/Transponder, die an oder in zu identifizierenden Abfallbehältern befestigt werden.
2	SW	c-secure vehicle Sicherheitsbibliothek der Fahrzeugsoftware	c-secure-vehicle.lib Version 2.0	Bei der Sicherheitsbibliothek handelt es sich um den EVG-Teil der Fahrzeugsoftware. Diese Sicherheitsbibliothek wird zusammen mit der Fahrzeugsoftware auf dem Fahrzeugrechner betrieben.
3	SW	c-secure office Sicherheitsmodul der Bürosoftware	c-secure-office.dll Version 2.0	Bei dem Sicherheitsmodul handelt es sich um den EVG-Teil der Bürosoftware. Das Modul wird als unabhängige Komponente in die Bürosoftware eingebettet, welche selbst nicht Bestandteil des EVG ist.

Tabelle 4: IT-Komponenten des EVG c-secure ident

Der Evaluierungsgegenstand hat

1. Eine Ausgangsschnittstelle des ID-Tags (unidirektional: Senden von Identifikationsdaten)
2. eine Schnittstelle in der Sicherheitsbibliothek „c-secure vehicle" der Fahrzeugsoftware (bidirektional: Empfang (aus Schnittstelle 1) und Austausch von Identifikationsdaten, Telematik-Ereignissen, Telematik-Uploads, Parametern, sowie weiteren Daten und Steuerkommandos),
3. eine Schnittstelle (bidirektional: Schreiben/Lesen von Telematik-Uploads) zu den Speichereinheiten auf dem Fahrzeugrechner,
4. eine Schnittstelle des Sicherheitsmoduls „c-secure office" der Bürosoftware (bidirektional: Automatisches Eingeben (der mittels Schnittstelle 3 geschriebenen und übertragenen Informationen) von Fahrzeugkennungen und ungeprüften Telematik-Uploads sowie anschließendes Zurückgeben von geprüften Telematik-Uploads und -Ereignissen).

Die Kanäle zwischen ID-Tag, Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware und Sicherheitsmodul c-secure office der Bürosoftware sind nicht Bestandteil des Evaluierungsgegenstands.

Weitere Schnittstellen, insbesondere die zur Clientkomponente der Bürosoftware und zu den kommunalen Abrechnungsstellen, sind nicht Bestandteil der Evaluierung.

Der EVG wird in folgendem Umfang ausgeliefert:

Nr.	Typ	Bezeichnung	Verweis / Version
1	HW	Transponder (ID-Tags)	Siehe Anhang „Transponder Übersicht“
2	SW	c-secure vehicle EVG-Teil der Fahrzeugsoftware	c-secure-vehicle.lib Version 2.0
3	DOK	Kurzanleitung c-ident 2 Bedienungsanleitung c-ident 2	[c-trace_Vehicle_kurz] [c-trace_Vehicle]
6	DOK	Transponder Übersicht für c-secure ident 2	[c-trace_Chip_Overview]
4	SW	c-secure office EVG-Teil der Bürosoftware	c-secure-office.dll Version 2.0
5	DOK	Benutzerhandbuch c-secure Office	[c-trace_Office]

Tabelle 5: Auslieferungsumfang des EVG

Logical Scope

In diesem Unterabschnitt werden die relevanten Sicherheitsfeatures der EVG-Komponenten für ein generelles Verständnis des Lesers in zusammenfassender Form definiert. Die nachfolgenden Unterpunkte orientieren sich an den drei definierten IT-Komponenten des EVG (vgl. Tabelle 4).

ID-Tag

Der Transponder (ID-Tag) übermittelt seine Identifikationsdaten (AT1) und die CRC-Prüfsumme an den RFID-Reader.

c-secure vehicle

Die Sicherheitsbibliothek c-secure vehicle berechnet anhand der Identifikationsdaten (AT1) vom ID-Tag die Prüfsumme und vergleicht diese mit der CRC-Prüfsumme aus dem ID-Tag. Das Ergebnis der Prüfung wird im Leerungsdatensatz (AT) abgespeichert (SF_ID_CHK). Desweitern wird dem Leerungsdatensatz die eindeutige Kennung des Fahrzeugsystems beigefügt (SF_KEN) und anschließend eine Prüfsumme über den Datensatz gebildet (SF_CRC_AT) und angehängt.

In regelmäßigen Abständen werden ein oder mehrere Leerungsdatensätze (AT) zu einem Leerungsdatenblock (AT+) zusammengefasst, über diesen Leerungsdatenblock wird eine Prüfsumme gebildet (SF_CRC_AT+). Die eindeutige Kennung des Fahrzeugsystems ist im Dateinamen des Leerungsdatenblocks abgebildet. Der Dateiname selbst liegt außerhalb von AT+ und wird über die Prüfsumme nicht abgesichert.

Der Leerungsdatenblock wird anschließend redundant abgespeichert (SF_SAVE) und auch dem Transferprogramm zum übertragen bereitgestellt.

c-secure office

Ziel der Sicherheitsfunktionen dieses Sicherheitsmodules ist es, die vom Fahrzeug erhaltenen Telematik-Uploads (AT+) und die darin enthaltenen Telematik-Ereignisse (AT) auf ihre Integrität hin zu prüfen und die Ergebnisse anschließend in der Datenbank zu persistieren, sodass der vertrau-

enswürdige Anwender die Möglichkeit hat, integre und nicht-integre Telematik-Uploads und Telematik-Ereignisse zu unterscheiden. Das Sicherheitsmodul prüft zum einen, ob die im Telematik-Upload gesetzte Fahrzeugkennung sowie die jeweils gesetzte Fahrzeugkennung der beinhalteten Telematik-Ereignissen valide ist. Weiterhin wird die Prüfsumme des Telematik-Uploads sowie die Prüfsummen der beinhalteten Telematik-Ereignisse im Sicherheitsmodul nachberechnet und mit den übermittelten Prüfsummen verglichen. Nur wenn Fahrzeugkennungen und Prüfsummen übereinstimmen, werden die Telematik-Uploads und Telematik-Ereignisse mit einem gültigen Ergebnis abgespeichert. Andernfalls werden sie als ungültig deklariert.

2 Postulate zur Übereinstimmung

Diese Sicherheitsvorgaben (Security Target – ST) und der EVG postulieren Übereinstimmung mit Common Criteria (CC) for IT Security Evaluation, Version 3.1, Revision 5 [CC].

Das ST und der EVG sind **CC Part 2 extended** mit Erweiterung um die Komponente

- FDP_ITT.5 "internal transfer integrity protection"

Das ST und der EVG sind **CC Part 3 conformant**.

Das ST und der EVG sind **EAL1 augmented** mit Anreicherung um die 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)

Das ST und der EVG sind **PP conformant** zum Schutzprofil

> „Protection Profile – Waste Bin Identification Systems, WBIS-PP",
> BSI-PP-0010-2004, Version 1.04 [WBIS-PP].

2.1 Art des EVG im WBIS-PP

Der EVG realisiert die gesamte Sicherheitsfunktionalität eines Abfall-Behälter-Identifikations-Systems (Waste Bin Identification System – WBIS). Die Angaben zur Art des EVG in Abschnitt 1.3 sind konsistent mit der Art des EVG im Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitte 1.2 und 8.2].

2.2 Definition des Sicherheitsproblems im WBIS-PP

Die Definition des Sicherheitsproblems in Abschnitt 3 dieser Sicherheitsvorgaben enthält alle Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken wie im Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitte 3 und 8.4] definiert.

Die Bedrohung T.Jam#1 und die organisatorische Sicherheitspolitik P.Safe wurden konkretisiert, um das Sicherheitsproblem zu verdeutlichen. Es wurden keine Annahmen, Bedrohungen oder organisatorische Sicherheitspolitiken hinzugefügt.

Anwendungshinweis 1 (AT: Leerungsdatensatz). Der Leerungsdatensatz AT wird innerhalb der im Fahrzeug installierten Komponenten des EVG, wie z.B. im Fahrzeugrechner oder im Leser, gebildet. Die Identifikationsdaten AT1 sind im ID-Tag gespeichert und bilden für sich ein schutzwürdiges Objekt bis zur Bildung des Datensatzes AT. Der Leerungsdatensatz AT kann optional weitere Datenfelder, wie z.B. Angaben zum Gewicht der Abfälle, enthalten.

Der Hinweis auf die Schutzwürdigkeit der Identifikationsdaten (AT1) ist in diese Sicherheitsvorgaben übernommen worden. Die Definition des Leerungsdatensatzes (AT) ist in diese Sicherheitsvorgaben übernommen und um weitere Datenfelder erweitert worden.

Anwendungshinweis 2 (AT+: Leerungsdatenblock). Ein Leerungsdatenblock (AT+) kann die gesamten Leerungsdatensätze einer Tour zusammenfassen.

Der Hinweis auf die Leerungsdatensätze einer Tour ist in diese Sicherheitsvorgaben nicht übernommen worden. Er ist nicht relevant, weil die Zusammenfassung in Leerungsdatenblöcke (AT+) unabhängig von der Tour erfolgt.

Anwendungshinweis 3 (S.Attack: Angreifer). Die Daten des Leerungsdatensatzes (AT) oder des Leerungsdatenblocks (AT+) können bei der Übertragung durch rein zufällige Einflüsse verfälscht werden. Solche Verfälschungen werden hier nicht als Bedrohungen angesehen, da kein Angreifer identifiziert werden kann. Die Wirksamkeit ggf. implementierter Funktionalität kann durch funktionale Tests (Bauartprüfung) nachgewiesen werden.

Der Hinweis auf die Möglichkeit der Verfälschung durch rein zufällige Einflüsse ist in diese Sicherheitsvorgaben nicht übernommen worden. Es ist nicht relevant, ob rein zufällige Verfälschungen (vgl. T.Man, T.Jam#1, T.Jam#2) durch Aktionen eines Angreifers (S.Attack) oder durch rein zufällige Einflüsse verursacht werden.

Anwendungshinweis 4 (T.Jam#2: Verfälschte Leerungsdatensätze). Es ist nicht möglich, die Angriffsmethoden genauer zu beschreiben, da diese stark von der Technik, die zur Implementierung des Datenkanals zwischen der Fahrzeugsoftware und dem Sicherheitsmodul verwendet wird, abhängen.

Der Hinweis ist in diesen Sicherheitsvorgaben berücksichtigt worden. Unabhängig von der Angriffsmethode führt jeder erfolgreiche Angriff immer zu rein zufälligen Verfälschungen. Für eine genauere Beschreibung der Angriffsmethoden besteht deshalb kein Bedarf.

Anwendungshinweis 5 (Bedrohungen). Der Autor der Sicherheitsvorgaben kann zusätzliche Bedrohungen aufnehmen, die das Produkt abwendet.

Der Hinweis ist in diesen Sicherheitsvorgaben berücksichtigt worden. Für die Aufnahme zusätzliche Bedrohungen besteht kein Bedarf.

Anwendungshinweis 6 (P.Safe: Fehlertoleranz). Die oben [in P.Safe] geforderte Funktionalität bezieht sich ausschließlich auf die Daten in der Fahrzeugsoftware. Diese Funktionalität muss mindestens bis zur vollständigen Übertragung in das Sicherheitsmodul, und damit in die Bürosoftware, sichergestellt werden. Es ist zu erwarten, dass der Schutz der Daten durch eine Datensicherung in einem sekundären Speicher des Fahrzeugrechners umgesetzt wird. Der Hersteller kann zusätzlich einen Zeitraum für diese Datensicherung im sekundären Speicher spezifizieren, so daß die Daten während dieses Zeitraums für eine wiederholte Übertragung zum Sicherheitsmodul verfügbar sind. Diese Datensicherungsfunktionalität schützt nicht gegen Datenverlust im Bürorechner (vgl. auch A.Backup).

Der Hinweis auf die Umsetzung der Fehlertoleranz durch Datenhaltung in einem sekundären Speicher ist bei der Ausgestaltung der EVG-Sicherheitsfunktionalität, wie in der EVG-Übersichtsspezifikation in Abschnitt 7 dieser Sicherheitsvorgaben dargelegt, berücksichtigt worden.

2.3 Sicherheitsziele im WBIS-PP

Die Darlegung der Sicherheitsziele in Abschnitt 4 dieser Sicherheitsvorgaben enthält alle Sicherheitsziele wie im Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitte 4 und 8.5] 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.

Zusätzlich sind die Sicherheitsanforderungen an die (Nicht-)IT-Umgebung aus dem Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitte 5.3 und 5.4] als Detaillierung der Sicherheitsziele für die Einsatzumgebung in Abschnitt 4.2 dieser Sicherheitsvorgaben übernommen worden.

Anwendungshinweis 7 (OT.Inv#1: Erkennung von ungültigen Identifikationsdaten). Die Sicherheitsziele fordern nur die Erkennung von z.B. fehlenden Daten im ID-Tag. Der EVG kann optional selbst auf solche erkannten Ereignisse reagieren. Da dies im Allgemeinen nicht umgesetzt sein wird, bleibt es dem Autor der Sicherheitsvorgaben überlassen, zusätzlich Sicherheitsziele für die Reaktion auf solche Ereignisse zu definieren.

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

2.4 Sicherheitsanforderungen im WBIS-PP

Die Darlegung der Sicherheitsanforderungen in den Abschnitten 5 und 6.1 dieser Sicherheitsvorgaben enthält alle Sicherheitsanforderungen an die Funktionalität wie im Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitte 5.1 und 6.4] definiert. Die Formulierung des Anforderungselements FDP_SDI.1.1 ist an die verwendete Ausgabe der Common Criteria (CC 3.1R5) angepasst worden.

Alle Operationen (Zuweisung, Auswahl) auf den Sicherheitsanforderungen sind in der vom Schutzprofil BSI-PP-0010-2004 vorgegebenen Art und Weise ausgeführt worden. Zusätzlich ist im Element FDP_SDI.1.1 eine redaktionelle Verfeinerung zur einheitlichen Verwendung des Begriffs ‚ID-Tag' ausgeführt worden.

Anwendungshinweis 8 (FDP_DAU.1: Einfache Datenauthentisierung). Es ist davon auszugehen, daß die obigen [in FDP_DAU.1 dargelegten] Anforderungen bei der beabsichtigten Vertrauenswürdigkeitsstufe der Evaluierung ohne Verwendung von Geheimnissen erfüllt werden können.

Der Hinweis auf die Erfüllbarkeit der Anforderungen an die Datenauthentisierung ohne Verwendung von Geheimnissen ist bei der Ausgestaltung der EVG-Sicherheitsfunktionalität, wie in der EVG-Übersichtsspezifikation in Abschnitt 7 dieser Sicherheitsvorgaben dargelegt, berücksichtigt worden.

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit sind nicht aus dem Schutzprofil BSI-PP-0010-2004 [WBIS-PP, Abschnitt 5.2] in den Abschnitt 6.2 dieser Sicherheitsvorgaben übernommen worden, bleiben aber so streng wie möglich an den Vorgaben der vorgeschriebenen Evaluierungsstufe EAL1. Dazu ist eine Anreicherung (Augmentierung) mit den Komponenten ASE_SPD.1, ASE_OBJ.2 (ersetzt ASE_OBJ.1) und ASE_REQ.2 (ASE_REQ.1) vorgenommen worden.

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

AT Ein Leerungsdatensatz AT zu einer Leerung eines Abfallbehälters ist ein schutzwürdiges Objekt im WBIS. Der Leerungsdatensatz AT besteht aus den folgenden Datenfeldern:

- **AT1** Identifikationsdaten des Abfallbehälters
- **AT2** Zeitstempel (Datum, Uhrzeit) des Leerungsvorgangs
- **AT3** Zusätzliche Daten zur Identifikation / Leerung (Ereignis- und Diagnoseinformationen, Gewicht, Status, …)
- **AT4** System-ID zur Identifikation des Fahrzeugs im Office
- **AT5** Ereigniszähler zur Vollständigkeitsprüfung der Datensätze

Der Leerungsdatensatz AT wird innerhalb der im Fahrzeug installierten Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware des EVG gebildet. Die Identifikationsdaten AT1 sind im ID-Tag gespeichert und bilden für sich ein schutzwürdiges Objekt bis zur Bildung des Datensatzes AT.

AT+ Vor der Übertragung von der Fahrzeugsoftware zum Sicherheitsmodul c-secure office werden die Leerungsdatensätze AT zu einem Leerungsdatenblock AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt im WBIS bei der Übertragung zwischen der Fahrzeugsoftware und dem Sicherheitsmodul c-secure office.

Subjekte

S.Trusted *Vertrauenswürdige Benutzer*

Die Besatzung des Fahrzeugs und die 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 Informationen der Anwendung zu modifizieren oder zu verfälschen. Der Angreifer verfügt höchstens über Kenntnisse offensichtlicher Schwachstellen.

3.1 Bedrohungen

Ein Angreifer benutzt die Schnittstellen des EVG mit dem Ziel, Schwachstellen auszunutzen. Dies führt zu einer beliebigen (rein zufälligen) Kompromittierung der Sicherheit des EVG. Die Bedrohungen adressieren alle Werte.

T.Man *Manipulierte Identifikationsdaten*

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

T.Jam#1 *Gestörte Identifikationsdaten*

Ein Angreifer (S.Attack) stört die Übertragung der Identifikationsdaten (AT1) im Fahrzeug vom ID-Tag zum Leser bzw. vom Leser zur Fahrzeugsoftware durch Mittel, z.B. elektromagnetische Strahlung, die die Identifikationsdaten (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 durch Mittel, z.B. elektromagnetische Strahlung, die die Daten der Leerungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen.

3.2 Organisatorische Sicherheitspolitiken

Die folgende Regel wird für den EVG formuliert:

P.Safe *Fehlertoleranz*

Die Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Speicherung der Daten in einem sekundären Speicher so gesichert sind, dass die Übertragung der Leerungsdatenblöcke

(AT+) von der Fahrzeugsoftware zum Sicherheitsmodul c-secure office im Fall des Verlusts von Leerungsdatenblöcke (AT+) im primären Speicher der Fahrzeugsoftware möglich ist.

3.3 Annahmen

A.Id *ID-Tag*

Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifikationsdaten (AT1) des Abfallbehälters sind im ID-Tag gespeichert. Es sind nur ID-Tags mit einmaligen Identifikationsdaten in Gebrauch. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist durch organisatorische Mittel außerhalb des EVG sicherzustellen.

A.Trusted *Vertrauenswürdiges Personal*

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

A.Access *Zugangsschutz*

Die Umgebung stellt durch geeignete Mittel (Verschluss, Zugangskontrolle durch Passwörter usw.) sicher, dass nur Benutzer oder Servicepersonal (S.Trusted) direkten Zugang zu allen Komponenten des EVG, außer zum ID-Tag, haben. Die Beeinflussung der internen Kommunikationskanäle durch potentielle Angreifer (S.Attack) innerhalb der IT-Struktur des Bürorechners ist durch angemessene Maßnahmen ausgeschlossen.

A.Check *Überprüfung der Vollständigkeit*

Der Benutzer (S.Trusted) kontrolliert in regelmäßigen Abständen, ob die vom Fahrzeugrechner zum Sicherheitsmodul im Büro übertragenen Benutzerdaten vollständig sind. Erkannte Datenverluste werden durch wiederholte Übertragung der Daten behoben. Die Abstände sind konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner.

A.Backup *Datensicherung*

Der Benutzer (S-Trusted) macht in regelmäßigen Abständen Sicherungskopien der vom EVG erzeugten Daten.

4 Sicherheitsziele

Dieser Abschnitt identifiziert und beschreibt die Sicherheitsziele für den EVG und seine Einsatzumgebung. Sicherheitsziele adressieren angemessen und vollständig das Sicherheitsproblem, d.h. sie sind geeignet, allen Bedrohungen entgegenzuwirken, alle organisatorischen Sicherheitspolitiken durchzusetzen und alle Annahmen aufrechtzuerhalten.

4.1 Sicherheitsziele für den EVG

OT.Inv#1 *Erkennung von ungültigen Identifikationsdaten*

Der EVG muss Manipulationen durch zufällige Störung an Identifikationsdaten (AT1) erkennen, die im ID-Tag gespeichert sind, oder während ihrer Übertragung im Fahrzeug vom ID-Tag zum Leser bzw. vom Leser zur Fahrzeugsoftware.

OT.Inv#2 *Erkennung von ungültigen Leerungsdatenblöcken*

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

OT.Safe *Fehlertoleranz*

Die Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Speicherung in einem sekundären Speicher so geschützt sind, dass die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul c-secure office bei einem Verlust der Leerungsdatenblöcke (AT+) im primären Speicher möglich ist.

4.2 Sicherheitsziele für die Umgebung

OE.ID *ID-Tag*

Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifikationsdaten (AT1) des Abfallbehälters sind im ID-Tag gespeichert. Es dürfen nur ID-Tags mit einmaligen Identifikationsdaten in Gebrauch sein. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist durch organisatorische Mittel außerhalb des EVG sicherzustellen.

Detaillierung (R.Id)

Der Benutzer muss folgendes sicherstellen: Der ID-Tag sollte an dem Abfallbehälter befestigt sein, der durch die in dem ID-Tag gespeicherten Identifikationsdaten zu identifizieren ist. Die in installierten ID-Tags gespeicherten Identifikationsdaten sind eindeutig. Die Zuordnung der Identifikationsdaten zum Gebührenpflichtigen muss durch organisatorische Mittel, welche nicht im Anwendungsbereich des EVG sind, erfolgen.

OE.Trusted *Vertrauenswürdiges Personal*

Es muss durch organisatorische Mittel sichergestellt sein, dass die Besatzung des Fahrzeuges und die Benutzer des Bürorechners (S.Trusted) autorisiert und vertrauenswürdig sind. Alle Personen, die das System installieren oder warten (S.Trusted), müssen autorisiert und vertrauenswürdig sein. Alle Personen, die für die Sicherheit der EVG-Umgebung verantwortlich sind (S.Trusted), müssen autorisiert und vertrauenswürdig sein.

Detaillierung (R.Trusted)

Die Personen, die das Fahrzeug und das Sicherheitsmodul betreiben, installieren und warten, müssen autorisiert und vertrauenswürdig sein. Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, sind autorisiert und vertrauenswürdig.

OE.Access *Zugangsschutz*

Die Umgebung muss durch geeignete Mittel (Verschluss, Zugangskontrolle durch Passwörter usw.) sicherstellen, dass nur Benutzer oder Servicepersonal (S.Trusted) direkten Zugang zu allen Komponenten des EVG, außer zum ID-Tag, haben. Die Beeinflussung der internen Kommunikationskanäle durch potentielle Angreifer (S.Attack) innerhalb der IT-Struktur des Bürorechners muss durch angemessene Maßnahmen ausgeschlossen sein.

Detaillierung (R.Access)

Die Umgebung muss durch geeignete Mittel sicherstellen, dass nur der Benutzer und das Servicepersonal direkten Zugang zu den Komponenten des EVG (außer zum ID-Tag) haben. Die Umgebung muss jedwede Beeinflussung der internen Datenkanäle innerhalb des Bürorechners verhindern.

OE.Check *Überprüfung auf Vollständigkeit*

Es muss sichergestellt sein, dass der Benutzer (S.Trusted) in regelmäßigen Abständen kontrolliert, ob die vom Fahrzeugrechner zum Sicherheitsmodul im Büro übertragenen Daten vollständig sind. Erkannte Datenverluste müssen durch wiederholte Übertragung der Daten behoben werden. Die Abstände müssen konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner sein.

Detaillierung (R.Check)

Der Benutzer muss in regelmäßigen Abständen die Vollständigkeit der Übertragung der Daten der Leerungsdatenblöcke (AT+) vom Fahrzeug zum Büro kontrollieren. Der Benutzer muss die Übertragung vom Fahrzeug zum Büro für die Daten anfordern, die von ihm als noch nicht übertragen festgestellt wurden, um den Verlust zu beheben. Die Zeitabstände der Benutzeraktionen für Kontrolle und Anforderung muss konsistent mit der verfügbaren Speicherkapazität sein, die durch den Fahrzeugrechner für den Zweck der Speicherung von Leerungsdatenblöcken (AT+) zur Verfügung gestellt wird.

OE.Backup *Datensicherung*

Es muss sichergestellt sein, dass der Benutzer (S-Trusted) in regelmäßigen Abständen Sicherheitskopien der vom EVG erzeugten Daten macht.

Detaillierung (R.Backup)

Der Benutzer muss die vom EVG erzeugten Daten in regelmäßigen Abständen in geeigneten Archiven sichern.

4.3 Erklärung der Sicherheitsziele

4.3.1 Rückverfolgung der Sicherheitsziele

Bedrohungen Politiken Annahmen	Sicherheitsziele							
	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						
P.Safe			x					
A.ID				x				
A.Trusted					x			
A.Access						x		
A.Check							x	
A.Backup								x

Tabelle 6: Rückverfolgung der Sicherheitsziele

4.3.2 Nachweis der Wirksamkeit gegen alle Bedrohungen

T.Man (Manipulierte Identifikationsdaten) behandelt Angriffe, in denen Identifikationsdaten (AT1) innerhalb des ID-Tags manipuliert werden. Entsprechend OT.Inv#1 werden die verfälschten Identifikationsdaten (AT1) durch den EVG erkannt (nachdem sie durch den Leser eingelesen worden sind), was der Bedrohung T.Man direkt entgegenwirkt.

T.Jam#1 (Gestörte Identifikationsdaten) behandelt Angriffe, in denen (durch zufällige Störung) verfälschte Identifikationsdaten (AT1) dem Leser bzw. der Fahrzeugsoftware übergeben werden. Entsprechend OT.Inv#1 werden die gestörten Identifikationsdaten durch den EVG erkannt (nachdem sie durch den Leser eingelesen worden sind), was der Bedrohung T.Jam#1 direkt entgegenwirkt.

T.Create (Ungültige Leerungsdatenblöcke) behandelt Angriffe, in denen beliebige Leerungsdaten erzeugt und dann an das Sicherheitsmodul übertragen werden. Entsprechend OT.Inv#2 wird jeder Versuch, beliebige (d.h. ungültige) Leerungsdatenblöcke an das Sicherheitsmodul zu übertragen, erkannt, was der Bedrohung T.Create direkt entgegenwirkt.

T.Jam#2 (Verfälschte Leerungsdatensätze) richtet sich auf Angriffe in denen Leerungsdatensätze (AT) während der Bearbeitung und Speicherung innerhalb des Fahrzeuges verfälscht werden oder die Übertragung der Leerungsdatenblöcke (AT+) zum Sicherheitsmodul gestört wird. Entsprechend OT.Inv#2 werden Verfälschungen von Leerungsdatensätzen während der Bearbeitung und Speicherung innerhalb des Fahrzeuges, und der Leerungsdatenblöcke, die während der Übertragung zum Sicherheitsmodul verfälscht werden, durch den EVG erkannt, was der Bedrohung T.Jam#2 direkt entgegenwirkt.

4.3.3 Nachweis der Durchsetzung aller organisatorischer Sicherheitspolitiken

P.Safe (Fehlertoleranz) sorgt für die Verfügbarkeit der relevanten Daten für die Übertragung der Leerungsdatenblöcke (AT+) von der Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware zum Sicherheitsmodul c-secure office, auch im Falle des Verlustes dieser Daten im Primärspeicher der Fahrzeugsoftware, indem die Daten im Sekundärspeicher gehalten werden. Dies wird exakt im Ziel OT.Safe wiederholt, so dass dieses Ziel hinreichend ist für die Durchsetzung von P.Safe.

4.3.4 Nachweis der Aufrechterhaltung aller Annahmen

A.Id (ID-Tag) stellt sicher, dass das ID-Tag am Abfallbehälter, welchen es identifiziert, befestigt ist, und die Daten des installierten ID-Tags einmalig sind. Die Übereinstimmung zwischen den Identifikationsdaten und dem Gebührenpflichtigen wird über organisatorische Mittel hergestellt. Da das Ziel OE.Id exakt dieselben Darlegungen enthält, ist es hinreichend für die Aufrechterhaltung von A.Id.

A.Trusted (Vertrauenswürdiges Personal) stellt sicher, dass alle Subjekte (außer dem Angreifer) vertrauenswürdig sind. Das Ziel OE.Trusted enthält exakt dieselben Darlegungen, so dass es hinreichend ist für die Aufrechterhaltung von A.Trusted.

A.Access (Zugangsschutz) stellt sicher, dass der Zugang zum EVG, außer zum ID-Tag, ausschließlich auf vertrauenswürdiges Personal beschränkt ist. Sie schließt ebenfalls die Fähigkeit des Angreifers aus, die internen Kommunikationskanäle innerhalb der IT-Struktur des Bürorechners zu beeinflussen. Das Ziel OE.Access enthält exakt dieselben Darlegungen, so dass es hinreichend ist für die Aufrechterhaltung von A.Access.

A.Check (Überprüfung der Vollständigkeit) stellt sicher, dass der Benutzer in regelmäßigen Intervallen prüft, ob die vom Fahrzeug zum Büro übertragenen Daten vollständig sind. Erkannte Datenverluste werden durch wiederholte Übertragung der Daten wiederhergestellt. Die Abstände sind konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner. Das Ziel OE.Check enthält exakt dieselben Darlegungen, so dass es hinreichend ist für die Aufrechterhaltung von A.Check.

A.Backup (Datensicherung) stellt sicher, dass der Benutzer in regelmäßigen Abständen Sicherungskopien der vom EVG erzeugten Daten anlegt, da der EVG keine entsprechende Funktion bereitstellt. Das Ziel OE.Backup enthält exakt dieselben Darlegungen, so dass es hinreichend ist für die Aufrechterhaltung von A.Backup.

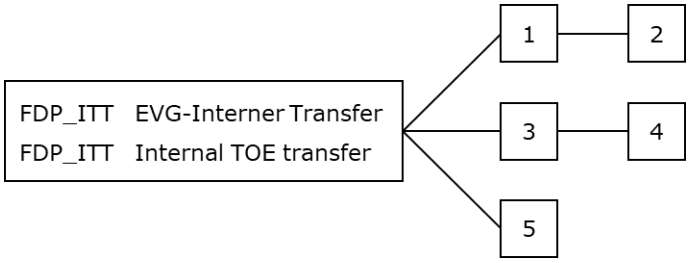
5 Definition erweiterter Komponenten

Zur Darlegung der Sicherheitsanforderungen an die Funktionalität des EVG wird eine zusätzliche Komponente (FDP_ITT.5) als Erweiterung der Familie FDP_ITT definiert. Diese Komponente beschreibt die Sicherheitsanforderungen an die Funktionalität für den Integritätsschutz von Benutzerdaten. Sie hat einen enger gefassten Ansatz als FDP_ITT.1, weil sie nicht unbedingt verlangt, dass der EVG funktionale Sicherheitspolitiken (Security Functional Policies SFPs) für Zugriffskontrolle und/oder Informationsflusskontrolle umsetzt, auch adressiert sie nur Manipulationen von Benutzerdaten.

FDP_ITT.5 wird definiert, weil Teil 2 der Common Criteria keine generische Sicherheitsanforderung an die Funktionalität für den Integritätsschutz von Benutzerdaten enthält, wenn sie zwischen materiell getrennten Teilen des EVG übertragen werden. Darüber hinaus hat FDP_ITT.5 einen enger gefassten Ansatz als FDP_ITT.1, denn es ist nicht unbedingt notwendig, daß der EVG funktionale Sicherheitspolitiken (Security Functional Policies SFPs) für Zugriffskontrolle und/oder Informationsflusskontrolle umsetzt, auch sind nur Manipulationen von Benutzerdaten adressiert.

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

Komponentenabstufung / Component levelling



FDP_ITT.5	Integritätsschutz des internen Transfers erfordert den Schutz von Benutzerdaten gegen Manipulationen bei der Übertragung zwischen Teilen eines 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.

Protokollierung / Audit: FDP_ITT.5

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

FDP_ITT.5	**Integritätsschutz des internen Transfers** Ist hierarchisch zu: Keinen anderen Komponenten. Abhängigkeiten: Keine Abhängigkeiten	**Internal transfer integrity protection** 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 materiell 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 Sicherheitsanforderungen

In diesem Kapitel sind die Sicherheitsanforderungen an die Funktionalität und die Vertrauenswürdigkeit des EVG dargelegt.

6.1 Sicherheitsanforderungen an die Funktionalität des EVG

Die Komponenten der Sicherheitsanforderungen an die Funktionalität (Security Functional Requirements – SFRs) des EVG sind aus Common Criteria [CC, Part 2] bezogen, mit Ausnahme der erweiterten Komponente FDP_ITT.5, die aus dem Schutzprofil BSI-PP-0010-2004 übernommen und in Abschnitt 5.1 definiert ist. Ausgeführte Operationen sind mit *Kursivschrift* ausgezeichnet.

6.1.1 Datenauthentisierung / Data authentication (FDP_DAU)

FDP_DAU.1	**Einfache Datenauthentisierung** **Basis data authentication**	
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 *Benutzer (S.Trusted)* die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten 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)

FDP_ITT.5 Integritätsschutz des internen Transfers
Internal transfer integrity protection

FDP_ITT.5.1	Die TSF müssen die *Datenintegritäts-politik* durchsetzen, um die Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen materiell getrennten Teilen des 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.
	Definition der Datenintegritätspolitik:	Definition of the Data Integrity Policy:
	Die Benutzerdaten (AT1 und AT+) müssen geschützt werden, um ihre Integrität zu erhalten.	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)

FDP_SDI.1 Überwachung der Integrität der gespeicherten Daten
Stored data integrity monitoring

FDP_SDI.1.1	Die TSF müssen die Benutzerdaten, die in Containern gespeichert sind, die von der TSF kontrolliert werden, auf *zufällige Manipulation* bei allen Objekten auf Basis folgender Attribute überwachen: *Identifikationsdaten AT1 innerhalb des ID-Tags und Leerungsdatensätze AT während der Speicherung im Fahrzeug*.	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 the ID tag and records of clearance AT during storage within the vehicle*.

6.1.4 Fehlertoleranz / Fault tolerance (FRU_FLT)

FRU_FLT.1 Verminderte Fehlertoleranz
Degraded fault tolerance

FRU_FLT.1.1	Die TSF müssen den Betrieb von *der Übertragung von Leerungsdatenblöcken (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gespeicherten Daten* sicherstellen, wenn die folgenden Fehler auftreten: *Verlust der Benutzerdaten 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 Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

Die Komponenten der Sicherheitsanforderungen an die Vertrauenswürdigkeit (Security Assurance Requirements – SARs) des EVG sind aus Common Criteria [CC, Part 3] bezogen.

Die folgende Tabelle enthält die Vertrauenswürdigkeitsklassen und -komponenten für die angestrebte Evaluierungsstufe EAL1 mit Anreicherung um ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2. Die Komponenten der Anreicherung (Augmentierung) sind mit **Fettschrift** ausgezeichnet.

Klasse	**Vertrauenswürdigkeitskomponenten**	
ADV	ADV_FSP.1	Einfache funktionale Spezifikation Basic functional specification
AGD	AGD_OPE.1	Benutzerhandbuch für den Betrieb Operational user guidance
	AGD_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

Tabelle 7: Anforderungen die Vertrauenswürdigkeit (EAL1 augmented)

6.3 Erklärung der Sicherheitsanforderungen

6.3.1 Rechtfertigung der Abhängigkeiten

Die Komponenten der Sicherheitsanforderungen an die Vertrauenswürdigkeit wurden genau wie durch EAL1 spezifiziert übernommen. Alle Abhängigkeiten innerhalb der Komponenten von EAL1 sind dadurch vollständig erfüllt.

Durch die Ergänzung der Evaluierungsstufe um die Vertrauenswürdigkeitskomponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 entstehen weitere Abhängigkeiten, die in der untenstehenden Tabelle betrachtet werden.

Die Abhängigkeiten der Sicherheitsanforderungen an die Funktionalität sind nicht vollständig erfüllt. Die nachstehende Tabelle bietet einen Überblick über die Abhängigkeiten und zeigt wie sie erfüllt sind.

Anforderungskomponente	Abhängigkeiten	Erfüllung
ASE_SPD.1	keine Abhängigkeiten	nicht anwendbar
ASE_OBJ.2	ASE_SPD.1	erfüllt
ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	erfüllt erfüllt
FDP_DAU.1	keine Abhängigkeiten	nicht anwendbar
FDP_ITT.5	keine Abhängigkeiten	nicht anwendbar
FDP_SDI.1	keine Abhängigkeiten	nicht anwendbar
FRU_FLT.1	FPT_FLS.1	siehe Besprechung unten

Tabelle 8: Abhängigkeiten der Sicherheitsanforderungen an die Funktionalität

FRU_FLT.1 fordert vom EVG, den Betrieb der Datenübertragung von der Fahrzeugsoftware zum Sicherheitsmodul sicherzustellen, selbst wenn die Daten innerhalb der Fahrzeugsoftware verloren gehen. Diese Anforderung wird verfolgt, um die organisatorische Sicherheitspolitik zu erfüllen, welche sich mehr auf die Verfügbarkeit von Daten bezieht, als auf korrekte Funktion der Software, und sich nicht auf einen sicheren Zustand des EVG bezieht, bezüglich der Bedrohungen, denen der EVG entgegenwirkt. Da sich die abhängige Komponente FPT_FLS.1 lediglich auf einen solchen sicheren Zustand des EVG (d.h. der Software) bezieht, ist sie für den EVG nicht anwendbar.

6.3.2 Rückverfolgung der Sicherheitsanforderungen an die Funktionalität

Komponente der Sicherheitsanforderungen an die Funktionalität	Sicherheitsziele für den EVG		
	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: Rückverfolgung der Sicherheitsanforderungen an die Funktionalität

6.3.3 Nachweis der Einhaltung der Sicherheitsziele für den EVG

OT.Inv#1 (Erkennung von ungültigen Identifikationsdaten) richtet sich auf das Erkennen von Manipulationen der Identifikationsdaten (AT1) innerhalb des ID-Tags und während sie zwischen dem ID-Tag und der Sicherheitsbibliothek c-secure vehicle der Fahrzeugsoftware, als materiell getrennten Teilen des EVG, übertragen werden. Der Schutz der Integrität der Identifikationsdaten (AT1), die im ID-Tag gespeichert sind, wird durch FDP_SDI.1 gefordert und wirkt zufälligen Manipulationen dieser Daten direkt entgegen. Der Schutz der Benutzerdaten AT1, um ihre Integrität sicherzustellen, wird durch FDP_ITT.5 für die Übertragung zwischen materiell getrennten Teilen des EVG gefordert. Die Datenintegrität sicherzustellen, schützt direkt vor zufälligen Manipulationen der Daten während des Transfers.

OT.Inv#2 (Erkennung von ungültigen Leerungsdatenblöcken) richtet sich auf das Erkennen von Manipulationen von Leerungsdatenblöcken (AT+), die zwischen der Fahrzeugsoftware und dem Sicherheitsmodul, als materiell getrennten Teilen des EVG, übertragen werden. Der Schutz der Benutzerdaten AT+, um ihre Integrität sicherzustellen, wird durch FDP_ITT.5 für die Übertragung zwischen materiell getrennten Teilen des EVG gefordert. Die Datenintegrität sicherzustellen, schützt direkt vor Manipulationen der Daten.

OT.Inv#2 richtet sich auch auf das Erkennen von ungültigen Leerungsdatensätzen AT während der Bearbeitung und Speicherung im Fahrzeug und Manipulationen von Leerungsdatenblöcken AT+, die zum Sicherheitsmodul übertragen werden. Der EVG stellt gemäß FDP_DAU.1 eine Fähigkeit bereit, einen Nachweis zu erzeugen, der vom Benutzer verwendet werden kann, um die Gültigkeit der Daten verifizieren. Der Schutz der Integrität der Benutzerdaten (AT), die im Fahrzeug gespeichert sind, wird durch FDP_SDI.1 gefordert und wirkt zufälligen Manipulationen dieser Daten direkt entgegen.

Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig bezüglich der Datenauthentisierung und -integrität. Daher decken die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 hinreichend das Sicherheitsziel OT.Inv#2 ab.

OT.Safe (Fehlertoleranz) richtet sich auf die Verfügbarkeit der relevanten Daten für die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul, selbst bei Datenverlust im primären Speicher der Fahrzeugsoftware. Der Betrieb dieser Datenübertragung mit Hilfe eines sekundären Speichers nach dem Verlust der Daten im primären Speicher wird gemäß FRU_FLT.1 durch den EVG ermöglicht.

6.3.4 Erläuterung der Sicherheitsanforderungen an die Vertrauenswürdigkeit

Die Vertrauenswürdigkeitsstufe für diesen EVG ist EAL1 augmented mit Anreicherung um ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2. Diese angereicherte Evaluierungsstufe bewirkt einen weitaus höheren Sicherheitsgrad gegenüber einem nicht-evaluierten IT-Produkt oder -System indem sie eine vertrauenswürdige Art der Bedienung vermittelt, während die Bedrohungen der Sicherheit nicht als ernst angesehen werden, was in direkter Beziehung zu dem eher niedrig anzusetzenden Wert der vom EVG zu schützenden Werte steht.

EAL1 mit der gewählten Anreicherung bietet unabhängige Vertrauenswürdigkeit um unterstützend dafür Sorge zu tragen, dass mit Informationen aus den Leerungsdatensätzen verantwortungsvoll umgegangen wird und dass der EVG einen den Kundenanforderungen angemessenen Schutz gegenüber bekannten Bedrohungen bietet.

Durch EAL1 mit der gewählten Anreicherung wird der EVG inklusive unabhängiger Tests der Sicherheitsfunktionalität und ausführlicher Untersuchung der bereitgestellten Anleitungen und Dokumentationen evaluiert. Die Anreicherung von EAL1 um die o.g. 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

Die Sicherheitsanforderungen an die Funktionalität des EVG werden durch folgende Sicherheitsfunktionen umgesetzt:

SF_ID_CHK ***(Umsetzung von FDP_SDI.1 und FDP_ITT.5)***

Funktion, die aufgrund von übergebenen Identifikationsdaten (AT1) aus dem Transponder (ID-Tag) mit anhängender Prüfsumme die Prüfsumme berechnet und das Ergebnis (gültig/ungültig) an den Leerungsdatensatz AT anhängt. Bei diesem Ergebnis handelt es sich um eine Information, ob die aus dem Transponder eingelesene Prüfsumme mit der durch den EVG berechneten Prüfsumme übereinstimmt.

SF_KEN ***(Umsetzung von FDP_DAU.1)***

Die Funktion, die in einen neu angelegten Leerungsdatensatz (AT) und einen neu angelegten Leerungsdatenblock (AT+) die Kennung des angeschlossenen Fahrzeugrechners schreibt.

SF_CRC_AT ***(Umsetzung von FDP_SDI.1)***

Die Funktion, die an einen Leerungsdatensatz AT eine Prüfsumme anhängt.

SF_CRC_AT+ *(Umsetzung von FDP_ITT.5)*

Die Funktion, die über einen Leerungsdatenblock AT+ eine Prüfsumme errechnet.

SF_SAFE *(Umsetzung von FRU_FLT.1)*

Die Funktion, die aus einer bestimmten Anzahl von Leerungsdatensätzen (AT) einen Leerungsdatenblock (AT+) zusammenstellt und diesen zusammen mit der von SF_KEN eingetragenen Kennung und der von SF_CRC_AT+ errechneten Prüfsumme im primären und sekundären Speicher ablegt.

SF_KEN_CHK *(Umsetzung von FDP_DAU.1)*

Die Funktion, die die Gültigkeit der Fahrzeugkennung im Leerungsdatensatz (AT) und im Leerungsdatenblock (AT+) prüft und das Ergebnis (gültig/ungültig) liefert. Bei diesem Ergebnis handelt es sich um eine Information, ob die auf dem Fahrzeugrechner in den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze eingetragenen Kennungen als gültige Kennungen konfiguriert sind. Die resultierende Information über die Gültigkeit wird vom Sicherheitsmodul c-secure office für die korrekte Weiterverarbeitung genutzt.

SF_AT_CHK_AT+_CHK *(Umsetzung von FDP_SDI.1 und FDP_ITT.5)*

Funktion, die aufgrund der von der Fahrzeugsoftware an das Sicherheitsmodul c-secure office übergebenen Leerungsdatenblöcke AT+ sowohl die Prüfsumme des Datenblocks (AT+) berechnet und das Ergebnis (gültig/ungültig) liefert, als auch die Prüfsumme für jeden im Datenblock enthaltenen Leerungsdatensatz (AT) berechnet und das Ergebnis (gültig/ungültig) liefert. Bei diesem Ergebnis handelt es sich um eine Information, ob die auf dem Fahrzeugrechner für den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze erzeugten Prüfsummen mit den berechneten Prüfsummen übereinstimmen. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheitsmodul c-secure office für die korrekte Weiterverarbeitung genutzt.

7.2 Einhaltung der Sicherheitsanforderungen an die Funktionalität

Die folgende Übersicht beschreibt, wie die Sicherheitsfunktionen auf die Sicherheitsanforderungen an die Funktionalität aus Kapitel 6.1 zurückgeführt werden können.

FDP_DAU.1.1 wird durch die Funktion SF_KEN erfüllt, weil durch das Auslesen der Kennung aus dem Fahrzeugrechner und das Einfügen in einen neu angelegten Leerungsdatensatz (AT) und einen neu angelegten Leerungsdatenblock (AT+) die geforderten Nachweise als Gültigkeitsgarantie erzeugt werden.

FDP_DAU.1.2 wird durch die Funktion SF_KEN_CHK erfüllt. Durch die Prüfung der Kennung des Fahrzeugrechners in einem Leerungsdatensatz AT bzw. Leerungsdatenblock AT+ erhält der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises.

FDP_ITT.5.1 Die zu schützenden Objekte sind AT1 während des Lesevorgangs und AT+ während der Übertragung zwischen EVG-Teil der Fahrzeugsoftware und Sicherheitsmodul.

Diese Anforderung wird für AT1 durch die Funktion SF_ID_CHK erfüllt, da durch die Überprüfung des CRC Wertes im ID-Tag sichergestellt ist, dass der Benutzer eine Veränderung der Daten AT1 beim Lesevorgang erkennen kann.

Für AT+ wird FDP_ITT.5 durch die Funktionen SF_CRC_AT+ und SF_AT_CHK_AT+_CHK erfüllt, weil durch die Erzeugung des CRC-Wertes als Integritätsmerkmal (SF_CRC_AT+) für einen Leerungsdatenblock (AT+) der Schutz der Benutzerdaten (AT+) vor Modifikation durchgesetzt wird, wenn diese zwischen der Fahrzeug-EVG-Komponente und der Bürorechner-EVG-Komponente übertragen werden. Durch die Überprüfung des CRC Wertes im Leerungsdatenblock (SF_AT_CHK_AT+_CHK) ist sichergestellt ist, dass der Benutzer eine Veränderung der Daten AT+ beim Übertragen in das Sicherheitsmodul erkennen kann.

FDP_SDI.1.1 Die zu schützenden Objekte sind AT1 innerhalb des ID-Tags und AT innerhalb des Fahrzeugspeichers.

Diese Anforderung wird für AT1 durch die Funktion SF_ID_CHK erfüllt, weil durch die Überprüfung des CRC Wertes im ID-Tag die Überwachung der Integrität von AT1 auf zufällige Manipulationen sichergestellt ist.

Für AT wird FDP_SDI.1 durch die Funktionen SF_CRC_AT und SF_AT_CHK_AT+_CHK erfüllt. SF_CRC_AT generiert das Integritätsmerkmal und SF_AT_CHK_AT+_CHK gewährleistet durch die Überprüfung dieses Merkmals die Überwachung der Integrität von AT während des gesamten Zeitraums der Speicherung im Fahrzeug auf zufällige Manipulationen.

FRU_FLT.1.1 Wird durch die Funktion SF_SAFE erfüllt, weil durch das Ablegen der Leerungsdatenblöcke (AT+) im Primär- und Sekundärspeicher die notwendige Voraussetzung geschaffen wird, dass bei einem Verlust von Benutzerdaten im Primärspeicher mit den im Sekundärspeicher gespeicherten Daten der Betrieb sichergestellt wird.

8 Literatur

[CC-Teil1] „Common Criteria for Information Technology Security Evaluation”,
Part 1: Introduction and general model, CCMB-2017-04-001
Part 2: Security functional components, CCMB-2017-04-002
Part 3: Security assurance components, CCMB-2017-04-003
Version 3.1, Revision 5, April 2017.

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

[c-trace_Vehicle_kurz] c-trace GmbH, „Kurzanleitung c-ident 2“, Version 2.04.

[c-trace_Vehicle] c-trace GmbH, „Bedienungsanleitung c-ident 2“, Version 2.08.

[c-trace_Chip_Overview] c-trace GmbH, „Transponder Übersicht für c-secure ident 2“, Version 1.5.

[c-trace_Office] c-trace GmbH, „Benutzerhandbuch c-secure-office 2.0“, Version 1.4.

9 Abbildungsverzeichnis

10 Tabellenverzeichnis

11 Mnemonics

AT	Leerungsdatensatz
AT+	Leerungsdatenblock
CHK	Check der Prüfsumme bzw. der Kennung
CRC	(Erzeugen einer) Prüfsumme
ID	Tag-ID
KEN	(Erzeugen einer) Kennung
SF	Sicherheitsfunktion

12 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CRC	Cyclic Redundancy Check
EAL	Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)
EVG	Evaluierungsgegenstand
FSP	Funktionale Spezifikation
IT	Informations-Technologie
OSP	Organisatorische Sicherheitspolitiken
PP	Protection Profile (Schutzprofil)
SFP	Security Function Policy (funktionale Sicherheitspolitik)
TOE	Target of Evaluation (Evaluierungsgegenstand)
TSC	TSF Scope of Control (Anwendungsbereich der TSF-Kontrolle)
TSF	TOE Security Functions (EVG-Sicherheitsfunktionen)
WBIS	Waste Bin Identification Systems (Abfallbehälter-Identifikations-System)

13 Anhang „Transponder Übersicht“

13.1 Zugelassene Transpondertypen

Dieser Anhang erläutert die technischen Kernparameter sowie die Bezeichnungen der Transpondertypen, die zur Herstellung eines BSI konformen Identifikationssystems c-ident zugelassen sind.

13.2 Transponder 125/134,2kHz

13.2.1 Transponder nach ISO 11784/11875

ISO 11784/11785 spezifiziert Transponder die in der Tieridentifikation eingesetzt werden.

ISO 11784 beschreibt ein einheitliches Nummerierungsschema (Bit Codierung) für die 64-Bit Transponder ID.

ISO 11785 beschreibt das Abfrageprotokoll für Full-Duplex (FDX) und Halb-Duplex (HDX) Transponder. In diesem Protokoll werden unter anderem die 64-Bit Transponder ID und eine 16 Bit Prüfsumme nach CCITT-CRC übertragen. Transponder ID und Prüfsumme sind im Read-Only Teil des Transponders gespeichert. Die Trägerfrequenz ist auf 134,2 kHz festgelegt.

Texas Instruments

RI-TRP-R9QL TRPGR30ATGA TRPGR30ATGB TRPGR30ATGC RI-INL-R9QM	Read-Only Transponder, HDX

EM MICROELECTRONIC

EM4005 EM4105	Read-Only Transponder, FDX

13.2.2 Transponder nach DIN EN 14803

DIN EN 14803 erweitert die ISO 11784 für das Anwendungsgebiet Entsorgungswirtschaft.

Texas Instruments

RI-TRP-0105 RI-TRP-0108 TRPGR30ENATGA TRPGR30ENATGB RI-INL-W007	Read-Only Transponder, HDX Nummernschema nach DIN EN 14803

EM MICROELECTRONIC

EM4305 EM4269 EM4369 EM4469 EM4569	Read-Write Transponder, gelockt auf Read-Only, FDX, Nummernschema programmiert nach DIN EN 14803

Silicon Craft

SIC7999	Read-Write Transponder, gelockt auf Read-Only, HDX, Nummernschema programmiert nach DIN EN 14803

13.3 Transponder 868 MHz

Transponder mit der Frequenz 868 MHz nach ISO/IEC 18000-63. Diese verfügen mindestens über eine feste 64bit Unique ID/OEM-Nummer und besitzen einen CRC.

Die DIN 30745 definiert das Nummernschema für die Entsorgungswirtschaft.

Impinj

Monza 4 Monza R6-P	Read-Write Transponder, gelockt auf Read-Only, Nummernschema programmiert nach DIN 30745

Änderungshistorie

Version	Datum	Autor	Änderung
1.0	3.2.2017	Ralf Bortfeldt	Urversion
1.1	8.2.2017	Ralf Bortfeldt	Prüfsumme eingeführt
1.2	9.2.2017	Ralf Bortfeldt	Namen der Security-Module eingesetzt
1.3	8.8.2017	Thomas Kemner	Diverse redaktionelle Änderungen aus Nachverfolgung übernommen
1.4	25.09.2017	Roland Vogt	Bearbeitung der Abschnitte 1, 2, 3, 4.1, 4,2, 5. Verschiebung der ‚Erklärungen' in die Abschnitte 4.3, 6.3.
1.5	28.09.2017	Roland Vogt	Bearbeitung der Abschnitte 4.3, 6, 7
1.6	06.12.2017	Thomas Kemner Felix Grumbach	Anhang „Transponder Übersicht" auf aktuellen Stand gebracht. Literaturverzeichnis aktualisiert. Abschnitt 3: Schutzwürdige Objekte AT1 bis AT5 definiert. Abbildung und Beschreibung in Abschnitt 1.4 überarbeitet
	06.02.2018	Thomas Kemner	Dokument entsprechend der Kommentare des Evaluators überarbeitet.
1.7	19.02.2018	Roland Vogt Thomas Kemner	Abschließende redaktionelle Bearbeitung aller Abschnitte zur Angleichung der deutschen Übersetzung an den englischen Wortlaut des Schutzprofils. [c-trace_User], [c-trace_Admin] sind das gleiche Dokument, Bearbeitung Abschnitt 1.4.
1.8	23.03.2018 - 13.04.2018	Thomas Kemner Felix Grumbach Ralf Grote	Überarbeitung der Abschnitte 1.3 und 1.4 gemäß Feststellungen der Evaluierung Wildcards in Transpondertypen entfernt und stattdessen explizite Typangabe.
1.9	20.07.2018	Thomas Kemner	Transponder-Typ Silicon Craft SIC799 zu Abschnitt 13 hinzugefügt. Update der Versionsnummern Abschnitt 8: [c-trace_Chip_Overview] und [c-trace_Office] Einige Überschriften tauchten ohne Nummerierung im Inhaltsverzeichnis auf => korrigiert. Abschnitt 1.5 – c-secure vehicle: Präzisierung Prüfsumme AT+.
1.10	10.09.2018	Ralf Grote	Nicht zulassungsfähige Transponder aus Abschnitt 13 entfernt. Update der Versionsnummern Abschnitt 8: [c-trace_Chip_Overview].
1.11	02.08.2019	Thomas Kemner	ST-Version und ST-Datum in Abschnitt 1.1 korrigiert. Nummerierung der Abschnitte „Schutzwürdige Objekte", „Subjekte" und „Angreifer" gelöscht.
1.12	12.08.2019	Thomas Kemner	Abschnitte 1.3.2, 1.4: Präzisierung Fahrzeugidentifikation als Gültigkeitsmerkmal.
1.13	25.02.2020	Sebastian Ahl-born	Aktualisierung der Version des c-secure office Benutzerhandbuches von Version 1.3 auf 1.4
1.14	09.03.2020	Thomas Kemner	Abschnitt „Andere Transponder" entfernt. Aktualisierung des Dokuments „Transponder-Übersicht" von Version 1.4 auf 1.5.