Sicherheitsvorgaben für c-trace Gefäßidentifikationssystem c-ident Version 1.0

c-trace GmbH
Westring 55
33818 Leopoldshöhe

Inhaltsverzeichnis

1 ST-Einführung

1.1 ST-Identifikation:

1	Titel:	Sicherheitsvorgaben für c-trace Gefäßidentifikationssystem c-ident Version 1.0
2	Editors:	Michael Eikelmann, c-trace GmbH
3	ST Version:	1.13
4	CC Version:	CC 2.3
5	Vertrauenswürdigkeitsstufe:	EAL1
6	Datum:	10.01.2008
7	EVG – Name:	c-ident
8	EVG – Version:	c-ident 1.0

1.2 ST-Übersicht:

9 Das Abfallbehälter-Identifikations-System wird im Bereich der Abfallentsorgung eingesetzt, wo Abrechnungssysteme gefordert werden, die eine verursacher- und mengengerechte Gebührenabrechnung ermöglichen. Das System ist so konzipiert, dass es völlig unabhängig 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.

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

11 Das Abfallbehälter-Identifikations-System prüft die vom Transponder eingelesenen Daten auf Integrität, ergänzt korrekte Daten durch Datum und Uhrzeit der Leerung, fügt ein Gültigkeits- sowie ein Integritätsmerkmal an und speichert diese Daten dann redundant auf zwei getrennten Speichern im Fahrzeugrechner, damit diese auch bei einem Datenverlust im ersten Speicher wieder hergestellt werden können. Vor der Übertragung in die Bürosoftware prüft das Abfallbehälter-Identifikations-System im Sicherheitsmodul die Daten erneut auf Gültigkeit und Integrität und kennzeichnet diese entsprechend.

12 Das Abfallbehälter-Identifikations-System gewährt Schutz vor Datenverlust und versehentlicher Datenverfälschung bis in die Bürosoftware.

13 Das Gefäßidentifikationssystem c-ident erfasst Abfallbehälter mit Hilfe der RFID - Technologie automatisch und zuverlässig. Ziel ist nicht nur, eine verursachergerechte Gebührenveranlagung gemäß einer vorgegebenen Satzung zu realisieren, 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.

14 Den Städten und Gemeinden bietet die Zertifizierung hinsichtlich der Daten- und Manipulationssicherheit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) die notwendige Sicherheit insbesondere beim gebührenrelevanten Einsatz von c-ident. Die Zertifizierung gemäß Protection Profile „Waste Bin Identification System (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.

15 Das Fahrzeug wird mit einem völlig neu konzipierten Identifikationssystem c-ident ausgestattet. Alle relevanten Daten werden darüber automatisch während der Entleerung erfasst.

16 Die Abfallbehälter werden mit einem Chip zur eindeutigen Zuordnung zum Eigentümer ausgerüstet. Hierzu stehen verschiedene Chiptypen in diversen Bauformen für die unterschiedlichsten Einsatzzwecke zur Verfügung.

17 Am Fahrzeug werden die Behälter eindeutig und sicher identifiziert und optional auch mit c-scale gewogen. Die Daten werden im EVG-Teil der Fahrzeugsoftware zu einem Leerungsdatenblock zusammengefasst und dann in das Sicherheitsmodul im Bürorechner übertragen und nach erfolgreicher Prüfung durch das Sicherheitsmodul der Büro-Software c-ware zur weiteren Verarbeitung bereitgestellt.

1.3 Postulat der Übereinstimmung mit den CC

18 Diese Sicherheitsvorgaben basieren auf den „Common Criteria“, Version 2.3 [CC-Teil1], [CC-Teil2], [CC-Teil3].

19 Entsprechend der in [CC-Teil1, Kap. 7.4] vorgesehenen Kennzeichnung werden folgende Aussagen zur Übereinstimmung mit den CC postuliert.

20 Der in Abschnitt 2 beschriebene Evaluationsgegenstand ist:

- **CC Part 2 extended.**

  Zusätzlich zu den aus Teil 2 der CC entnommenen und in Kap. 5.1.1 beschriebenen funktionalen Anforderungen wird „FDP_ITT.5“ verwendet. Diese funktionale Anforderung ist nicht aus den CC, Version 2.3, entnommen aber wird in [BSI-PP0010] explizit dargelegt und ebenfalls in Kap. 5.1.1 beschrieben.

- **CC Part 3 conformant.**

  Die Konformität ist durch die in Kap. 5.1.2 beschriebene Auswahl von Vertrauenswürdigkeitskomponenten aus Teil 3 der CC gewährleistet.

- **EAL1 conformant.**

  Die Konformität ist durch die in Kap. 5.1.2 beschriebene Auswahl der Evaluierungsstufe EAL1 und der entsprechenden Vertrauenswürdigkeitskomponenten aus Teil 3 der CC gewährleistet.

- **PP conformant**

  Der EVG ist konform zum Schutzprofil, „Protection Profile – Waste Bin Identification Systems, WBIS-PP“, Version 1.04 [BSI-PP0010].

2 EVG-Beschreibung

21 Der EVG heißt c-ident, Version 1.0, bestehend aus dem Software-Modul IWS_BSI.OBJ Version 1.1, c-secure.exe Version 1.1, sowie den dazugehörigen Transpondern (ID-Tags).

22 Er besteht aus folgenden Komponenten:

Nr.	Typ	Bezeichnung	Version	Anmerkung
1	HW	Transponder (ID-Tags)	Siehe Anhang „Transponder Übersicht"	Bei den ID-Tags handelt es sich um passive Transponder, die am oder im zu identifizierenden Gegenstand befestigt werden.
2	SW	EVG-Teil der Fahrzeugsoftware	IWS_BSI.obj Version 1.1 Dateien: IWS_BSI.C Version 1.1 IWS_BSI.H Version 1.1	Anmerkung: Diese Library wird zusammen mit der Firmware auf einem von der Firma c-trace entwickelten Fahrzeugrechner betrieben, basierend auf einem 32 Bit Mikroprozessor der ARM7 Familie von Philips.
3	SW	Sicherheitsmodul	c-secure.exe Version 1.1	Bei dem Sicherheitsmodul handelt es sich um den EVG-Teil der Bürosoftware. Dieses Modul ist unabhängig von der Bürosoftware, die nicht Bestandteil des EVG ist.

Tabelle 1: Komponenten des EVG

23 Die folgende Abbildung gibt einen Überblick über das Abfallbehälter-Identifikations-System.

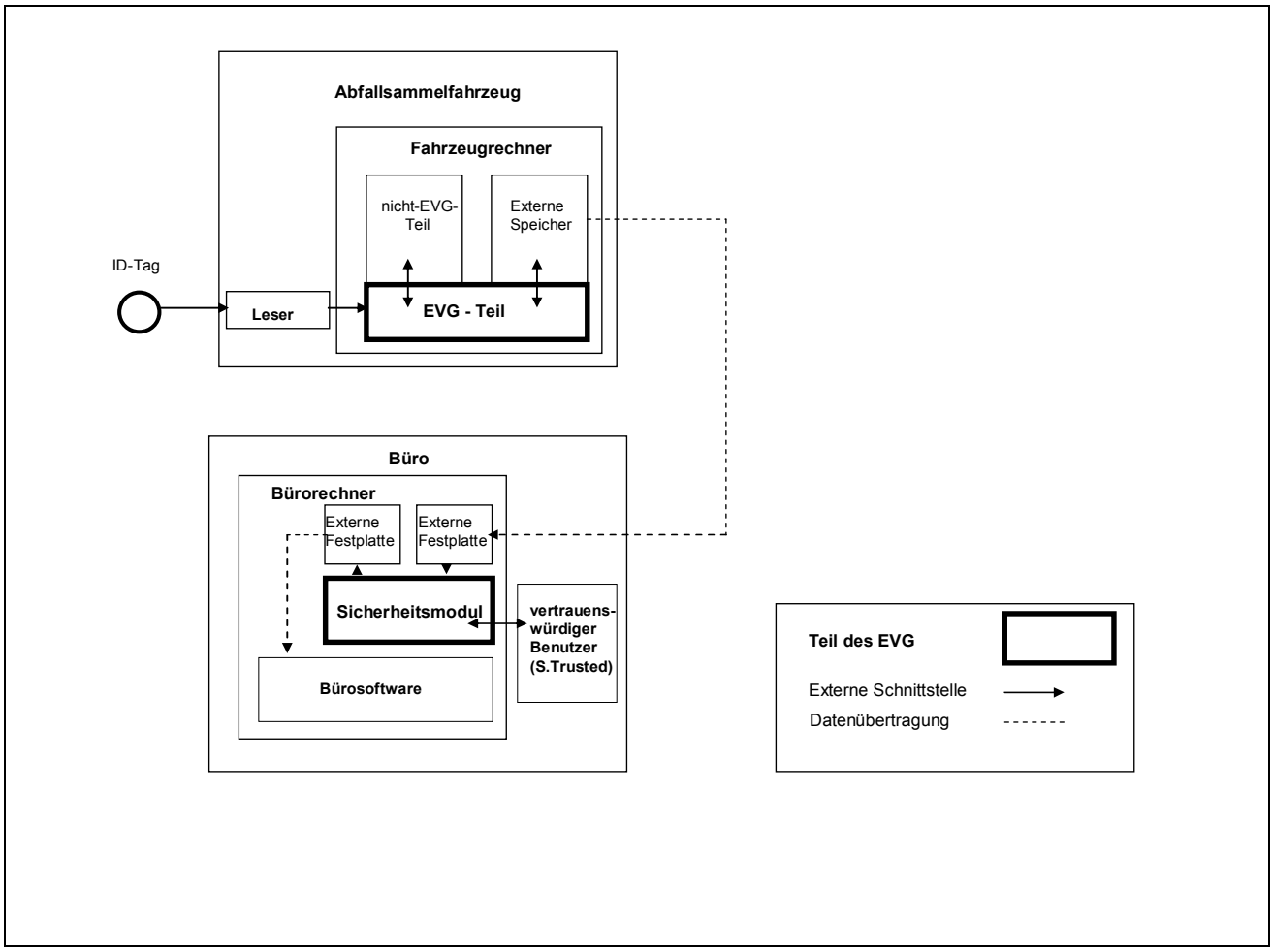

Abbildung 1: Abfallbehälter-Identifikations-System

24 Das System besteht aus drei getrennten Teilen. Dies sind die Transponder (ID-Tag) gemäß Anhang „Transponder Übersicht“ mit den Identifikationsdaten, das Abfallsammelfahrzeug mit dem Fahrzeugrechner und der Bürorechner mit der Bürosoftware. Der Fahrzeugrechner beinhaltet den EVG-Teil der Fahrzeugsoftware, den nicht-EVG-Teil der Fahrzeugsoftware und die externen Speicher, die ebenfalls nicht zum EVG gehören. Die Bürosoftware auf dem Bürorechner ist nicht Bestandteil des EVG. Das Sicherheitsmodul ist ein eigenständiges Programm auf dem Bürorechner. Der Bürorechner verfügt über eine externe Festplatte zum Empfang der Leerungsdaten und zur Archivierung der geprüften Leerungsdaten. Die EVG-Teile sind in der Abbildung durch dicke schwarze Rahmen und die verschiedenen Schnittstellen der EVG-Teile durch schwarze Pfeile gekennzeichnet.

25 Das Abfallbehälter-Identifikations-System 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.

26 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 ent-

halten, um auch zur gewichtsbezogenen Abrechnung benutzt zu werden. Andere ergänzende Verfahren sind in der Zukunft möglich.

27 Die Abfallbehälter werden mit einem Datenträger (ID-Tag) ausgestattet. Der ID-Tag speichert Identifikationsdaten, die zur Identifizierung 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 Reader ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden erkannt. Die Identifikationsdaten werden dann an die Fahrzeugsoftware weitergeleitet. Optional wird 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. Der nicht EVG-Teil der Fahrzeugsoftware ergänzt diese Daten um Datum- und Zeitangaben. Der EVG-Teil der Fahrzeugsoftware fügt ein Gültigkeits- sowie ein Integritätsmerkmal an und bildet daraus einen Leerungsdatensatz.

28 Ein oder mehrere Leerungsdatensätze werden zu einem Leerungsdatenblock zusammengefasst. Es können auf diese Weise alle Leerungsdatensätze einer Tour zu einem „Touren-Datenblock“ zusammengefasst werden.

29 Die Leerungsdatenblöcke werden vom nicht EVG-Teil der Fahrzeugsoftware über das Sicherheitsmodul im Bürorechner an die Bürosoftware übertragen. Der EVG-Teil der Fahrzeugsoftware sorgt durch geeignete Maßnahmen dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist. Bei der Übermittlung der Leerungsdatenblöcke an die Bürosoftware wird durch das Sicherheitsmodul sichergestellt, dass nur die in einem Fahrzeug, das zu diesem WBIS gehört, erstellten Datenblöcke als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt.

30 Die Leerungsdatenblöcke können von der Bürosoftware in dem Bürorechner gespeichert werden. Sie können optional ausgewertet werden. Die Leerungsdatensätze, die in den Datenblöcken enthalten sind, oder die Datenblöcke selbst werden an externe Systeme (z.B. bei den Kommunen) zur Abrechnung mit dem Kunden weitergeleitet.

31 Der ID-Tag und die Datenübertragungsstrecke zwischen dem ID-Tag und der Fahrzeugsoftware, die im Fahrzeug gespeicherten Daten sowie die Übertragungsstrecke zwischen der Fahrzeugsoftware und dem Sicherheitsmodul 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 mit dem Bürorechner realisiert.

Nr.	Typ	Bezeichnung	Version
1	HW	Transponder (ID-Tags)	Siehe Anhang „Transponder Übersicht“
2	SW	EVG-Teil der Fahrzeugsoftware	IWS_BSI.OBJ Version 1.1 Dateien: IWS_BSI.C Version 1.1 IWS_BSI.H Version 1.1
3	DOK	Systemverwalterhandbuch Fahrzeug Benutzerhandbuch Fahrzeug	[c-trace_Ident], [c-trace_Terminal], [c-trace_boardPC] [c-trace_Ident_kurz]
4	SW	Sicherheitsmodul	c-secure.exe 1.1
5	DOK	Systemverwalterhandbuch Office Benutzerhandbuch Office	[c-trace_Admin] [c-trace_User]
6	DOK	Transponder Übersicht für c-ident 1.0	Siehe Anhang „Transponder Übersicht“

Tabelle 2: Auslieferungsumfang des EVG

2.1 Abgrenzung des Evaluierungsgegenstandes

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

33 Der EVG beinhaltet die Softwarekomponente IWS_BSI.OBJ Version 1.1 als Teil der Fahrzeugsoftware. Der EVG-Teil der Fahrzeugsoftware prüft die vom Transponder eingelesenen Daten auf Integrität. Daraufhin werden korrekte Daten im nicht-EVG-Teil der Fahrzeugsoftware um Datum und Uhrzeit der Leerung ergänzt. Der EVG-Teil der Fahrzeugsoftware fügt dann ein Gültigkeits- sowie ein Integritätsmerkmal an und speichert diese Daten redundant auf zwei Speichern im Fahrzeugrechner. Jegliche weitere Funktionalität der Fahrzeugsoftware ist nicht Bestandteil der Zertifizie-

rung. Die Speicher gehören ebenfalls nicht zum EVG. Die Speicher sind zwei SD/MMC Karten. Die eine Karte wird als Primärspeicher und andere Karte als Sekundärspeicher eingesetzt.

34 Die Daten werden über ein GSM/GPRS Modem an das Sicherheitmodul übertragen (Die Daten können per Wählverbindung oder über das Internet übertragen werden). Die Modemverbindung ist nicht Bestandteil der Zertifizierung.

35 Des Weiteren beinhaltet der EVG das Sicherheitsmodul, die Software-Komponente c-secure.exe Version 1.1. Das Sicherheitsmodul prüft die Daten erneut auf Gültigkeit und Integrität und kennzeichnet diese entsprechend für die Weiterverarbeitung. Die Bürosoftware ist nicht Bestandteil der Zertifizierung.

36 Ebenfalls zum EVG gehören die Transponder (ID-Tags), die im Anhang „Transponder Übersicht“ beschrieben werden.

37 **Der Evaluierungsgegenstand hat folgende externe Schnittstellen:**

I.1. Eine unidirektionale Schnittstelle zwischen dem ID-Tag und dem Leser. Sie ist unidirektional, da nur Daten vom Transponder zum Leser gelangen.

I.2. Eine unidirektionale Schnittstelle zwischen dem Leser und dem EVG-Teil der Fahrzeugsoftware. Sie ist unidirektional, da die Leser Daten über den CAN-Bus an den EVG-Teil der Fahrzeugsoftware schicken.

I.3. Eine bidirektionale Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem nicht-EVG-Teil der Fahrzeugsoftware. Sie ist bidirektional, weil Leerungsdatensätze AT, Leerungsdatenblöcke AT+, Parameter sowie optionale Daten und Steuerkommandos zwischen den beiden Teilen ausgetauscht werden.

I.4. Eine bidirektionale Schnittstelle zwischen EVG-Teil der Fahrzeugsoftware und den externen Speichern. Sie ist bidirektional, da Leerungsdatensätze AT auf die externen Speicher übertragen und wieder gelesen werden.

I.5. Eine bidirektionale Schnittstelle zwischen externer Festplatte des Bürorechners und dem Sicherheitsmodul. Sie ist bidirektional, da das Sicherheitsmodul die Leerungsdatenblöcke (AT+) von der externen Festplatte liest und wieder auf die Festplatte zurück schreibt. Während der Prüfung werden die gültigen und integren Leerungsdatenblöcke (AT+) und die darin enthaltenen Leerungsdatensätze (AT) in ein für die Bürosoftware lesbares Datenformat konvertiert. Die von der Fahrzeugsoftware generierten Leerungsdatenblöcke (AT+) sind in einem nicht für die Bürosoftware lesbaren Datenformat auf der externen Festplatte gespeichert. Darüber hinaus werden eine Liste gültiger Fahrzeugkennungen und die Protokolldaten der Prüfergebnisse auf der externen Festplatte gespeichert.

I.6. Eine bidirektionale Benutzerschnittstelle zwischen Sicherheitsmodul und vertrauenswürdigem Benutzer S.Trusted zur Ausgabe der Betriebsmodi, Fehlermeldungen und Prüfergebnissen, sowie zur Eingabe der Konfigurationsdaten des Sicherheitsmoduls. Über die Benutzerschnittstelle wird auch die Liste gültiger Fahrzeugkennungen eingegeben.

38 Die physischen Kanäle zwischen den Komponenten des EVG, ID-Tag – Fahrzeugsoftware – Sicherheitsmodul, also die Übertragungswege von Schnittstelle zu Schnittstelle, sind nicht Bestandteil des EVG. Ebenso ist die Bürosoftware kein Bestandteil des EVG.

3 EVG-Sicherheitsumgebung

39 Nachfolgend werden zunächst die schutzwürdigen Objekte, die Subjekte und die Urheber von Bedrohungen definiert.

40 **Schutzwürdige Objekte:**

41 **AT** Ein Leerungsdatensatz AT zu einer Leerung ist ein schutzwürdiges Objekt in einem WBIS. Ein Leerungsdatensatz AT besteht aus den Datenfeldern:

42 **AT1** Identifikationsdaten des Abfallbehälters

43 **AT2** Zeitstempel (Datum, Uhrzeit, optional GPS-Koordinaten) des Leerungsvorgangs

44 **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.

45 **Subjekte:**

46 **S.Trusted** *Vertrauenswürdige Benutzer*

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

48 **Angreifer:**

49 **S.Attack** *Angreifer*

50 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

51 **A.Id:** *ID-Tag*

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

53 **A.Trusted:** *Vertrauenswürdiges Personal*

54 Die Besatzung des Fahrzeuges und die Benutzer des Bürorechners (S.Trusted) sind autorisiert

und vertrauensvoll. Alle Personen, die das System installieren, initialisieren oder warten sind autorisiert und vertrauenswürdig (S.Trusted). Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, (S.Trusted), sind autorisiert und vertrauenswürdig.

55 **A.Access:** *Zugangsschutz*

56 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 potentiellen Angreifer (S.Attack) innerhalb der IT – Struktur des Bürorechners ist aufgrund geeigneter Maßnahmen ausgeschlossen.

57 **A.Check** *Check of completeness*

58 Der Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle Daten von dem Fahrzeugrechner in das Sicherheitsmodul übertragen wurden (Vollständigkeit der Übertragung). Erkannte Datenverluste werden vom Benutzer (S.Trusted) 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 Leerungsdaten zur Verfügung steht.

59 **A.Backup:** *Datensicherung*

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

61 **A.Installation:** *Systeminstallation*

62 Bei Installation des Identifikationssystems auf dem Fahrzeug wird sichergestellt, dass die Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

3.2 Bedrohungen

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

64 **Aufgrund der obigen Definitionen wurden folgende Bedrohungen identifiziert, denen der EVG entgegenwirken muss:**

65 **T.Man** *Manipulierte Identifikationsdaten*

66 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.

67 **T.Jam#1** *Gestörte Identifikationsdaten*

68 Ein Angreifer (S.Attack) stört die Übertragung der Identifizierungsdaten AT1 vom ID-Tag zum Leser im Fahrzeug durch Mittel (z.B. elektronische Strahlung), die die Identifizierungsdaten AT1 ausschließlich rein zufällig verfälschen.

69 **T.Create** *Ungültige Leerungsdatenblöcke*

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

71 **T.Jam#2** *Verfälschte Leerungsdatensätze*

72 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

73 **In Ergänzung zur Abwehr der Bedrohung soll der EVG die folgende Sicherheitspolitik unterstützen:**

74 **P.Safe** *Fehlertoleranz*

75 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

76 Für den angenommenen Einsatz werden die folgenden Bedrohungen angenommen:

- Absichtliche oder unabsichtliche Unterdrückung oder Verfälschung der im ID-Tag gespeicherten Identifikationsdaten durch Mülltonnenbesitzer, Nachbarn, Fremde mittels Manipulation am Transponder der Mülltonne.
- Verfälschung oder Unterdrückung der Identifizierungsdaten AT1 aufgrund eines Übertragungsfehlers zwischen Transponder und Fahrzeugrechner.
- Versehentliche Verfälschung oder Unterdrückung der Leerungsdatenblöcke AT+ zwischen Fahrzeugrechner und Sicherheitsmodul auf dem Bürorechner.
- Verlust aller Leerungsdatenblöcke AT+ einer Tour durch Verlust oder Beschädigung während der Datenübertragung auf den Bürorechner.

4.1 Sicherheitsziele für den TOE (EVG)

77 **OT.Inv#1** *Erkennung von ungültigen Identifikationsdaten*

78 Der EVG soll Manipulationen an Identifikationsdaten erkennen (AT1), die in einem ID-Tag gespeichert sind, oder während sie zwischen ID-Tag und Leser im Fahrzeug übertragen werden.

79 **OT.Inv#2** *Erkennung von ungültigen Leerungsdatenblöcken*

80 Er soll Manipulationen an empfangenen Leerungsdatensätzen während des Leerungsprozesses und Speicherns im Fahrzeug erkennen, sowie Manipulationen der Leerungsdatenblöcke bei zufälligen Störungen während des Transfers von der Fahrzeugsoftware zum Sicherheitsmodul. Er soll jeden Versuch einer Übermittlung willkürlicher (z.B. ungültiger) Leerungsdatenblöcke an das Sicherheitsmodul erkennen.

81 **OT.Safe** *Fehlertoleranz*

82 Der EVG soll sicherstellen, dass die Daten redundant in einem sekundären Speicher gesichert werden. So ist der Transfer der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul auch noch möglich, wenn Daten in einem der beiden Speicherkarten verloren gehen.

4.2 Sicherheitsziele für die Umgebung

83 **OE.ID** *ID-Tag*

84 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.

85 **OE.Trusted** *Vertrauenswürdiges Personal*

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

87 **OE.Access** *Zugangsschutz*

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

89 **OE.Check** *Überprüfung auf Vollständigkeit*

90 Der Benutzer prüft in regelmäßigen Abständen, ob alle Leerungsdatensätze von dem Fahrzeugrechner komplett übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer (S.Trusted) in einem bestimmten Zeitraum durch erneutes Abrufen beim Fahrzeugrechner behoben.

91 **OE.Backup** *Datensicherung*

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

93 **OE.Installation** *Installation*

94 Bei Installation des Identifikationssystems auf dem Fahrzeug wird sichergestellt, dass die Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation als auch im Service- / Wartungsfall.

5 IT - Sicherheitsanforderungen

95 Die im Schutzprofil ausgewählten und in die Sicherheitsvorgaben übernommenen funktionalen Sicherheitsanforderungen (SFR – Security Functional Requirements) sind CC, Teil 2 erweitert.

5.1 EVG – Sicherheitsumgebung

96 Da der EVG vor allem gegen unabsichtliche oder zufällige Veränderungen und Verluste von Daten, z.B. durch technische Effekte, wie Handystrahlung, wirkt, genügt für seine Prüfung zunächst die Vertrauenswürdigkeitsstufe EAL1. Diese enthält keine Familien der Klasse AVA, insbesondere keine Komponenten der Familie AVA-SOF „Stärke der Sicherheitsfunktionen“. Postulate zur EVG-Funktionsstärke sind somit nicht erforderlich.

5.1.1 Funktionale Sicherheitsanforderungen an den TOE (EVG)

Funktionale Sicherheitsanforderung	**Bedeutung**
FDP	Schutz der Benutzerdaten
FDP_DAU.1	Einfache Datenauthentisierung
FDP_SDI.1	Überwachung der Integrität der gespeicherten Daten
FRU	Betriebsmittelnutzung
FRU_FLT.1	Verminderte Fehlertoleranz

Tabelle 3: SFRs des EVG CC, Teil 2 konform

97 **Data authentication (FDP_DAU)**

98 **Basis data authentication (FDP_DAU.1)**

99 FDP_DAU.1.1 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+***[1]

100 FDP_DAU.1.2 The TSF shall provide ***user (S.Trusted)***[2] with the ability to verify evidence of the validity of the indicated information

101 **Stored data integrity (FDP_SDI)**

102 **Stored data integrity monitoring (FDP_SDI.1)**

103 FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for ***random manipulation***[3] on all objects, based on the following attributes: ***identification data AT1 within identification unit and records of clearance AT during storage within the vehicle***[4].

104 **Fault tolerance (FRU_FLT)**

105 **Degraded fault tolerance (FRU_FLT.1)**

106 FRU_FLT.1.1 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***[5] when the following failures occur: ***Loss of user data in the primary memory of the vehicle software***[6].

107 Die Auflistung in Tabelle 4 zeigt die explizit dargelegten (Teil 2 erweiterten) SFRs:

Funktionale Sicherheitsanforderung	**Bedeutung**
FDP	Schutz der Benutzerdaten
FDP_ITT.5	Interne Transferintegrität

Tabelle 4: SFRs des EVG CC, Teil 2 erweitert

[1] assignment: *list of objects or information types*

[2] assignment: *list of subjects*

[3] assignment: *integrity errors*

[4] assignment: *user data attributes*

[5] assignment: *list of TOE capabilities*

[6] assignment: *list of type of failures*

108 **Internal TOE transfer (FDP_ITT)**

109 **Internal transfer integrity protection** (FDP_ITT.5) (Common Criteria Part 2 extended)

110 FDP_ITT.5.1 The TSF shall enforce the ***Data Integrity Policy***[1] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

111 The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement "Internal transfer integrity protection (FDP_ITT.5)":

112 The User Data (AT1 and AT+) shall be protected in order to maintain its integrity

5.1.2 Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

113 Die Vertrauenswürdigkeitsstufe EAL1 wird angestrebt, und es ergeben sich folgende Anforderungen

114 Übersicht über die Vertrauenswürdigkeitsstufe EAL1:

Sicherheitsklasse	**Sicherheitsbestandteile**	**Bedeutung**
Konfigurationsmanagement	ACM_CAP.1	Versionsnummer
Auslieferung und Betrieb	ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
Entwicklung	ADV_FSP.1 ADV_RCR.1	Informelle funktionale Spezifikation Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1 AGD_USR.1	Systemverwalterhandbuch Benutzerhandbuch
Testen	ATE_IND.1	Unabhängiges Testen

Tabelle 5: Anforderungen an die Vertrauenswürdigkeit nach EAL1

5.2 Sicherheitsanforderungen an die IT-Umgebung

115 Es werden keine Sicherheitsanforderungen an die IT – Umgebung gestellt.

[1] assignment: *Integrity SFP(s)*

5.3 Sicherheitsanforderungen an die nicht IT-Umgebung

116 **R.Id** *ID-Tag*

117 Der Benutzer muss folgendes sicherstellen: Der ID-Tag muss am Abfallbehälter befestigt sein, damit er identifiziert werden kann. Die Identifikationsdaten des ID-Tags müssen eineindeutig sein. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.

118 **R.Trusted** *Vertrauenswürdiges Personal*

119 Alle Personen, die das System installieren oder warten sind autorisiert und vertrauenswürdig. Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, sind autorisiert und vertrauenswürdig.

120 **R.Access** *Zugangsschutz*

121 Die Umgebung stellt durch geeignete Maßnahmen sicher, dass nur die Benutzer bzw. das Servicepersonal den direkten Zugang zu allen Komponenten des EVG haben. Die Beeinflussung der internen Verbindungskanäle ist durch geeignete Maßnahmen ausgeschlossen.

122 **R.Check** *Überprüfung der Vollständigkeit*

123 Der Benutzer 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 Leerungsdatensätze (AT) zur Verfügung steht.

124 **R.Backup** *Datensicherung*

125 Der Benutzer sichert die vom Evaluierungsgegenstand erzeugten Daten regelmäßig im Archiv.

126 **R.Installation:** *Systeminstallation*

127 Das Servicepersonal stellt bei der Installation des Identifikationssystems auf dem Fahrzeug sicher, dass die Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

6 EVG – Übersichtsspezifikation

6.1 EVG – Sicherheitsfunktionen

128 Die funktionalen Sicherheitsanforderungen des TOE (EVG) werden durch folgende Sicherheitsfunktionen umgesetzt:

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

130 Funktion, die aufgrund von übergebenen Identifikationsdaten (AT1) aus dem Transponder (ID-Tag) mit anhängendem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) an den nicht-EVG-Teil der Fahrzeugsoftware übergibt. Bei diesem Ergebnis handelt es sich um eine Information, ob der aus dem Transponder eingelesene CRC-Wert mit dem aktuellen durch den EVG berechneten CRC-Wert übereinstimmt.

131 SF_CRC_AT *(Umsetzung von FDP_SDI.1)*

132 Die Funktion, die an einen Leerungsdatensatz AT einen CRC-Wert anhängt.

133 SF_CRC_AT+ *(Umsetzung von FDP_ITT.5)*

134 Wird eine Übertragung der Leerungsdaten angestoßen, sammelt der EVG eine bestimmte Anzahl von Leerungsdatensätzen (AT) zu einem Leerungsdatenblock (AT+) zusammen. Über diesen Leerungsdatenblock (AT+) wird von der Funktion ein CRC-Wert anhängt.

135 SF_KEN *(Umsetzung von FDP_DAU.1)*

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

137 SF_SAFE *(Umsetzung von FRU_FLT.1)*

138 Die Funktion, die die Leerungsdatensätze (AT) im primären und sekundären Speicher ablegt und wieder ausliest.

139 SF_KEN_CHK *(Umsetzung von FDP_DAU.1)*

Die Funktion, die die Gültigkeit der Fahrzeugkennung im Leerungsdatensatz (AT) und im Leerungsdatenblock (AT+) prüft.

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

141 Funktion, die aufgrund der vom EVG-Teil der Fahrzeugsoftware an das Sicherheitsmodul übergebenen Leerungsdatenblöcke AT+ mit beigefügtem CRC-Wert sowohl den CRC-Wert des Datenblocks (AT+) berechnet und das Ergebnis (gültig/ungültig) anzeigt, als auch den CRC-Wert für je-

den im Datenblock enthaltenen Leerungsdatensatz (AT) berechnet und das Ergebnis (gültig/ungültig) anzeigt. Bei diesem Ergebnis handelt es sich um eine Information, ob der auf dem Fahrzeugrechner für den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze AT erzeugten CRC-Werte mit den aktuellen, durch den EVG berechneten CRC-Werten übereinstimmen. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheitsmodul für die korrekte Weiterverarbeitung genutzt.

142 Die folgende Tabelle gibt eine Übersicht darüber, wie die Sicherheitsfunktionen auf die funktionalen Sicherheitsanforderungen aus Kapitel 5.1.1 zurückgeführt werden können.

SF_ID_CHK	Funktion, die aufgrund von übergebenen Identifikationsdaten (**AT1**) aus dem Transponder (ID-Tag) mit anhängendem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) an den nicht-EVG-Teil der Fahrzeugsoftware übergibt. Bei diesem Ergebnis handelt es sich um eine Information, ob der aus dem Transponder eingelesene CRC-Wert mit dem aktuellen durch den EVG berechneten CRC-Wert übereinstimmt	
	FDP_SDI.1	FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for random manipulation on all objects, based on the following attributes: identification data **AT1** within identification unit and records of clearance AT during storage within the vehicle.
	FDP_ITT.5	FDP_ITT.5.1 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. The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement “Internal transfer integrity protection (FDP_ITT.5)”: The User Data (**AT1** and AT+) shall be protected in order to maintain its integrity
SF_CRC_AT	Die Funktion, die an einen Leerungsdatensatz **AT** einen CRC-Wert anhängt.	
	FDP_SDI.1	FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for random manipulation on all objects, based on the following attributes: identification data AT1 within identification unit and records of clearance **AT** during storage within the vehicle.
SF_CRC_AT+	Wird eine Übertragung der Leerungsdaten angestoßen, sammelt der EVG eine bestimmte Anzahl von Leerungsdatensätzen (AT) zu einem Leerungsdatenblock (AT+) zusammen. Über diesen Leerungsdatenblock **(AT+)** wird von der Funktion ein CRC-Wert anhängt.	
	FDP_ITT.5	FDP_ITT.5.1 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.

		The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement “Internal transfer integrity protection (FDP_ITT.5)”: The User Data (AT1 and **AT+**) shall be protected in order to maintain its integrity
SF_AT_CHK_AT+_CHK	Funktion, die aufgrund der vom EVG-Teil der Fahrzeugsoftware an das Sicherheitsmodul übergebenen Leerungsdatenblöcke AT+ mit beigefügtem CRC-Wert sowohl den CRC-Wert des Datenblocks (**AT+**) berechnet und das Ergebnis (gültig/ungültig) anzeigt, als auch den CRC-Wert für jeden im Datenblock enthaltenen Leerungsdatensatz (**AT**) berechnet und das Ergebnis (gültig/ungültig) anzeigt. Bei diesem Ergebnis handelt es sich um eine Information, ob der auf dem Fahrzeugrechner für den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze AT erzeugten CRC-Werte mit den aktuellen, durch den EVG berechneten CRC-Werten übereinstimmen. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheitsmodul für die korrekte Weiterverarbeitung genutzt	
	FDP_SDI.1	FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for random manipulation on all objects, based on the following attributes: identification data AT1 within identification unit and records of clearance **AT** during storage within the vehicle.
	FDP_ITT.5	FDP_ITT.5.1 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. The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement “Internal transfer integrity protection (FDP_ITT.5)”: The User Data (AT1 and **AT+**) shall be protected in order to maintain its integrity
SF_KEN	Die Funktion, die in einen neu angelegten Leerungsdatensatz (**AT**) und einen neu angelegten Leerungsdatenblock (AT) die Kennung des angeschlossenen Fahrzeugrechners schreibt	
	FDP_DAU.1	FDP_DAU.1.1 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+**.
SF_KEN_CHK	Die Funktion, die die Gültigkeit der Fahrzeugkennung im Leerungsdatensatz **(AT**) und im Leerungsdatenblock **(AT+)** prüft.	
	FDP_DAU.1	FDP_DAU.1.2 The TSF shall provide user (S.Trusted) with the ability to verify evidence of the validity of the indicated information
SF_SAFE	Die Funktion, die die Leerungsdatensätze (AT) im **primären und sekundären**	

	Speicher ablegt und wieder ausliest.	
	FRU_FLT.1	FRU_FLT.1.1 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.

Tabelle 6: Abdecken der funktionalen Sicherheitsanforderungen durch die EVG-Sicherheitsfunktionen

6.2 Maßnahmen zur Vertrauenswürdigkeit

143 **ACM_CAP.1** *Konfigurationsmanagement*

144 Der Verweisname lautet: c-ident 1.0 und für jede weitere Version eindeutig. Die Teilsysteme des EVG sind mit den in Tabelle 1 aufgeführten Verweisnamen und Versionsnummern gekennzeichnet.

145 **ADO_IGS.1** *Installations,- Generierungs- und Anlaufprozeduren*

146 In den Systemverwalterhandbüchern sind die Installationsanweisungen und Generierungen für den sicheren Anlauf des EVG beschrieben.

147 Alle Schritte für die sichere Installation und Generierung des EVG sind im Systemverwalterhandbuch beschrieben.

148 **Familie ADV (ADV_FSP.1 / ADV_RCR.1)** *Informelle funktionale Spezifikation und Informeller Nachweis der Übereinstimmung*

149 Es wird eine Beschreibung der funktionalen Spezifikation konsistent zu der EVG-Übersichtsspezifikation bereitgestellt, zusammen mit einem informellen Nachweis der Übereinstimmung zur EVG-Übersichtsspezifikation.

150 **AGD_ADM.1** *Systemverwalterhandbuch*

151 Mit dem EVG wird folgende Dokumentation ausgeliefert:

- Systemverwalterhandbuch Fahrzeug für die Fahrzeugausstattung: [c-trace_Ident], [c-trace_Terminal], [c-trace_boardPC];
- Systemverwalterhandbuch Office für die Büroausstattung: [c-trace_Admin].

152 Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Installation und Bedienung des EVG.

153 **AGD_USR.1** *Benutzerhandbuch*

154 Mit dem EVG wird folgende Dokumentation ausgeliefert:

- Benutzerhandbuch Fahrzeug für die Fahrzeugausstattung: [c-trace_Ident_kurz];
- Benutzerhandbuch Office für die Büroausstattung: [c-trace_User].

155 Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Bedienung des EVG.

156 **ATE_IND.1** *Unabhängiges Testen*

157 Das Testsystem besteht aus einer Nachbildung eines Fahrzeugsystems, einem PC als Testrechner, auf dem verschiedene Testsoftware zur Auswertung des Tests installiert sind. Auf dem PC ist ebenfalls das Sicherheitsmodul installiert. Es werden Transponder entsprechend der Transponder-Übersicht im Anhang eingesetzt.

158 Das nachgebildete Fahrzeugsystem besteht aus folgenden Teilen:

- Fahrzeugrechner CIR mit dem CanOpen (normiert als CleanOpen) Netzwerk
- Schüttungsterminal zur Anzeige von Informationen
- Identifikationseinheit (Leser) inkl. Kammhakenantenne
- GSM / GPRS Modem zur Übertragung der Leerungsdaten

159 Das Testsystem wird dem Evaluator zur Verfügung gestellt.

7 PP – Postulate

7.1 PP – Verweis

160 Der EVG ist konform zu „Protection Profile Waste Bin Identifikation System WBIS-PP Version 1.04“ [BSI-PP0010]. Er erfüllt daher alle Anforderungen des WBIS-PP, Version 1.04.

7.2 PP – Anpassung

161 Keine Anpassungen vorgenommen.

7.3 PP – Ergänzungen

162 Gegenüber dem WBIS-PP, Version 1.04, wurden die folgenden Annahmen, Ziele und Anforderungen ergänzt:

- Annahme A.Installation, vergleiche Abschnitt 3.1
- Ziel OE.Installation, vergleiche Abschnitt 4.2
- Anforderung R.Installation, vergleiche Abschnitt 5.3

8 Erklärungen

8.1 Erklärung der Sicherheitsziele

163 Zuordnung zu den Sicherheitszielen

Threats - Assumptions – Policies / Security objektives	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						

Tabelle 7: Sicherheitsziele

164 Die Erklärung für diese Zuordnungen werden im Schutzprofil [BSI-PP0010] im Abschnitt 6.2.2.1, “policies and security objectives sufficiency”, im Abschnitt 6.2.2.2, “threats and security objective sufficiency”, und im Abschnitt 6.2.2.3 “assumptions and security objective sufficiency” vollständig und hinreichend erklärt. Die Annahme A.Installation, sowie das Ziel an die Umgebung OE.Installation wurden ergänzt. Dabei ist OE.Installation eindeutig auf A.Installation zurück verfolgbar und geeignet, A.Installation vollständig abzudecken.

8.2 Erklärung der Sicherheitsanforderungen

165 Funktionale Sicherheitsanforderung zum Sicherheitsziel

TOE Security Functional Requirement / TOE Security objectives	OT.Inv#1	OT.Inv#2	OT.Save
FDP_DAU.1		x	
FDP_ITT.5	x	x	
FDP_SDI.1	x	x	
FDP_FLT.1			x

Tabelle 8: Security Functional Requirement to TOE Security Objective Mapping

166 Sicherheitsanforderung der Umgebung zum Sicherheitsziel der Umgebung

Enviroment Security Requirement / TOE Security objectives	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

Tabelle 9: Environment security requirement to Environment Security Objective Mapping

8.2.1 Erklärung der internen Konsistenz und gegenseitigen Unterstützung

167 Die interne Konsistenz und gegenseitige Unterstützung werden im Kapitel 6.3 des Schutzprofils [BSI-PP0010] erklärt.

8.2.2 Erklärung der Vertrauenswürdigkeitsstufe

168 Die Wahl der Vertrauenswürdigkeitsstufe wird im Schutzprofil [BSI-PP0010] Im Abschnitt 6.6 folgendermaßen erklärt: „The assurance level for this protection profile is EAL1. This EAL provides a meaningful increase in assurance over an unevaluated IT product or system by providing confidence in correct operation, while the threats to security are not viewed as serious, which relates di-

rectly to the rather low value of the TOE's assets. EAL1 provides independent assurance to support the contention that due care has been exercised with respect to the protection of information contained in records of clearance and that the TOE provides useful protection against identified threats as required by the customer. EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. This enables the required flexibility in composing the system of modules taken from the current market, while keeping the associated costs for the evaluation at reasonable low level."

8.2.3 Erklärung zu den Abhängigkeiten

169 Die Abhängigkeiten werden im Schutzprofil [BSI-PP0010] wie folgt genau erklärt:

170 "The security assurance components are taken exactly as specified by EAL1. All dependencies are therefore completely fulfilled.

171 The functional requirements dependencies for the TOE and for the environment are not completely fulfilled. The following table gives an overview of the dependencies and shows how they are fulfilled.

Requirement	Dependencies	Fulfilled
FDP_DAU.1	no dependencies	implicitly
FDP_ITT.5	no dependencies	implicitly
FDP_SDI.1	no dependencies	implicitly
FRU_FLT.1	FPT_FLS.1	see discussion below

Tabelle 10: Functional Requirements Dependencies

172 FRU_FLT.1 requires the TOE to ensure the operation of the data transfer from the vehicle software to the security module even if the data is lost within the vehicle software. This requirement is driven to fulfil the organisational security policy, which relates more to the availability of the data then to the correct functionality of the software and does not relate to a secure state of the TOE in terms of the threats the TOE is countering. As the dependency component FPT_FLS.1 relates merely to such secure state of the TOE (i.e. the software) it is not applicable for the TOE."

8.3 Erklärung der EVG – Übersichtsspezifikation

8.3.1 Erklärung der IT-Sicherheitsfunktionen

173 Die Kombination der IT-Sicherheitsfunktionen wirkt so zusammen, dass die funktionalen Anforderungen aus Kapitel 5.1.1 erfüllt werden. Dies wird im Folgenden begründet:

Sicherheitsfunktionen / Sicherheitsanforderungen	FDP_DAU.1	FDP_SDI.1	FDP_ITT.5	FRU_FLT.1
SF_ID_CHK		x	x	
SF_CRC_AT		x		
SF_CRC_AT+			x	
SF_KEN	x			
SF_SAFE				x
SF_KEN_CHK	x			
SF_AT_CHK_AT+_CHK		x	x	

Tabelle 11: Übersicht der Sicherheitsfunktionen zu den Sicherheitsanforderungen

174 **FDP_DAU.1**

175 Wird durch die Funktion SF_KEN erfüllt, weil durch das sofortige Auslesen der Kennung aus dem Fahrzeugrechner und das sofortige Einfügen in einen neu angelegten Leerungsdatensatz (AT) und einen neu angelegten Leerungsdatenblock (AT+) die notwendige Voraussetzung geschaffen wird, dass der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises erhält. FDP_DAU wird durch die Funktion SF_KEN_CHK erfüllt. Durch die Prüfung der Kennung des Fahrzeugrechners, in einem AT, erhält der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises. Durch Prüfung der Kennung des Fahrzeugrechners in einem AT+ erhält der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises eines AT+.

176 **FDP_SDI.1**

177 Die zu schützenden Objekte sind AT1 innerhalb der Identifikationseinheit und AT innerhalb des Fahrzeugspeichers.

178 Diese Anforderung wird für AT1 durch die Funktion SF_ID_CHK erfüllt, weil durch die Überprüfung des CRC Wertes im ID-Tag sichergestellt ist, dass der Benutzer eine zufällige Manipulation der Identifikationsdaten (AT1) erkennen kann.

179 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 bietet durch Überprüfen dieses Merkmals dem Benutzer die Möglichkeit zur Feststellung der zufälligen Manipulation bei Aufzeichnung der Leerungsdatensätze (AT) während des Speicherns innerhalb des Fahrzeuges erhält.

180 **FDP_ITT.5**

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

182 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.

183 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.

184 **FRU_FLT.1**

185 Wird durch die Funktion SF_SAFE erfüllt, weil durch das Ablegen der Leerungsdatensätze (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.

8.3.2 Erklärung der Funktionsstärke

186 Die Anforderungen an die Vertrauenswürdigkeit enthalten nicht die Komponente AVA_SOF.1. Deshalb ist es nicht erforderlich eine Funktionsstärke zu postulieren.

8.3.3 Erklärung der Vertrauenswürdigkeitsmaßnahmen

187 Die in Abschnitt 6.2 formulierten Vertrauenswürdigkeitsmaßnahmen erfüllen alle in Abschnitt 5.1.2 identifizierten Anforderungen an die Vertrauenswürdigkeit des EVG, gemäß den CC, Teil3 [CC-Teil3]. (vgl.Tabelle 12):

Anforderungen gemäß EAL1	**Maßnahmen des Herstellers**
Konfigurations-management : ▪ ACM_CAP.1	Der Verweisname lautet: c-ident 1.0 und für jede weitere Version eindeutig. Die Teilsysteme des EVG sind mit den in Tabelle 1 aufgeführten Verweisnamen und Versionsnummern gekennzeichnet.
Auslieferung und Betrieb: ▪ ADO_IGS.1	In den Systemverwalterhandbüchern Fahrzeug und Office sind die Installationsanweisungen und Generierungen für den sicheren Anlauf des EVG beschrieben. Alle Schritte für die sichere Installation und Generierung des EVG sind im Systemverwalterhandbuch beschrieben.

Anforderungen gemäß EAL1	Maßnahmen des Herstellers
Entwicklung: ▪ ADV_FSP.1 ▪ ADV_RCR.1	Es wird eine Beschreibung der funktionalen Spezifikation konsistent zu der EVG-Übersichtsspezifikation bereitgestellt, zusammen mit einem informellen Nachweis der Übereinstimmung zur EVG-Übersichtsspezifikation.
Handbücher: ▪ AGD_ADM.1 ▪ AGD_USR.1	Mit dem EVG wird folgende Dokumentation ausgeliefert: ▪ Systemverwalterhandbuch Fahrzeug für die Fahrzeugausstattung: [c-trace_Ident], [c-trace_Terminal], [c-trace_boardPC]; ▪ Systemverwalterhandbuch Office für die Büroausstattung: [c-trace_Admin]. Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Installation und Bedienung des EVG. Mit dem EVG wird folgende Dokumentation ausgeliefert: ▪ Benutzerhandbuch Fahrzeug für die Fahrzeugausstattung: [c-trace_Ident_kurz]; ▪ Benutzerhandbuch Office für die Büroausstattung: [c-trace_User]. Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Bedienung des EVG.
Testen: ▪ ATE_IND.1	Das Testsystem besteht aus einer Nachbildung eines Fahrzeugsystems, einem PC als Testrechner, auf dem verschiedene Testsoftware zur Auswertung des Tests installiert sind. Auf dem PC ist ebenfalls das Sicherheitsmodul installiert. Es werden Transponder entsprechend der Transponder-Übersicht im Anhang eingesetzt.

Tabelle 12: Realisierung der Anforderungen an die Vertrauenswürdigkeit

8.4 Erklärung der PP – Postulate

188 Der EVG ist konform zum „Protection Profile Waste Bin Identifikation Systems WBIS-PP Version 1.04 [BSI-PP0010]".

189 Der EVG ist erweitert um die Annahme A.Installation, das Ziel an die EVG-Umgebung OE.Installation und die Anforderung R.Installation.

9 Literatur

[CC-Teil1] Common Criteria, „Common Criteria for Information technology security evaluation, Part 1: Introduction and general model“, Version 2.3, August 2005.

[CC-Teil2] Common Criteria, „Common Criteria for Information technology security evaluation, Part 2: Security functional requirements“, Version 2.3, August 2005.

[CC-Teil3] Common Criteria, „Common Criteria for Information technology security evaluation, Part 3: Security assurance requirements“, Version 2.3, August 2005.

[BSI-PP0010] Deutscher Städte und Gemeindebund, Bundesamt für Sicherheit in der Informationstechnik (BSI), „Protection Profile – Waste Bin Identification Systems, WBIS-PP“, Version 1.04, Mai 2004.

[Transponder Übersicht] c-trace GmbH, „Transponder Übersicht für c-ident 1.0“, Version 1.3.

[c-trace_Ident_kurz] c-trace GmbH, „c-ident Kurzbedienungsanleitung“, Version 1.2.

[c-trace_Ident] c-trace GmbH, „Bedienungsanleitung c-trace Identsystem c-ident“, Version 1.11

[c-trace_Admin] c-trace GmbH, „Systemverwalterhandbuch c-secureoffice 1.1 zum Sicherheitsmodul c-secure.exe Version 1.1“, Version 1.5.

[c-trace_User] c-trace GmbH, „Benutzerhandbuch c-secureoffice 1.1 zum Sicherheitsmodul c-secure.exe Version 1.1“, Version 1.5.

[c-trace_Terminal] c-trace GmbH, „Technisches Handbuch zum c-trace Bedienterminal CTERM CR1050“, Version 1.6.

[c-trace_boardPC] c-trace GmbH, „Technisches Handbuch zum c-trace Identrechner CIR“, Version 1.4.

10 Anhang „Transponder Übersicht“

10.1 Zugelassene Transpondertypen

190 Dieser Anhang erläutert die technischen Kernparameter sowie die Bezeichnungen der Transpondertypen, die zur Herstellung eines BSI konformen Identifikationssystems c-ident 1.0 zugelassen sind.

10.2 Transponder nach ISO 11784/11875 und DIN EN 14803

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

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

193 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 (AT1) 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.

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

195 Transpondertypen die diesen Normen entsprechen:

Texas Instruments

196 RI-TRP-xxxx (x = beliebig)

197 z.Bsp. RI-TRP-RR2B RI-TRP-RE2B RI-TRP-RRHP RI-TRP-REHP RI-TRP-R9WK RI-TRP-DR2B

198 RI-TRP-IR2B

EM MICROELECTRONIC

199 EM4005, EM4105, EM4369, EM4569

ATMEL/TEMIC

200 e5530, TK5551, ATA5567(T5557), ATA5570

NXP/Philips Semiconductors

201 Hitag-2, Hitag-S

10.3 Transponder nach ISO 11875 ohne Nummernschema

202 Transponder analog 10.2, allerdings entspricht die Transponder ID nicht der DIN EN 14803 bzw. der ISO 11784.

10.4 4 MHz Transponder

203 4 MHz MIDAT 2-kBit IMES

204 4 MHz MIDAT 4-kBit CoCoS

205 Read-Write Transponder mit fester 32 Bit Transponder ID und CRC.

10.5 Andere Transponder 125/134,2 kHz

206 Transponder im Frequenzbereich von 125-134,2 kHz, die nicht alle Anforderungen von ISO 11784/11875 und DIN EN 14803 erfüllen, die aber mindestens über eine feste 32/40/64 Bit Unique ID/OEM-Nummer verfügen und einen CRC besitzen.

Texas Instruments

207 RI-TRP-Mxxx (x = beliebig)

NXP/Philips Semiconductors

208 Hitag-1