Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1063-2020

zu

c-secure-ident, Version 2.0

der

c-trace GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1063-2020 (*)

Abfallbehälter-Identifikationssystem

c-secure-ident, Version 2.0

von	c-trace GmbH
PP-Konformität:	Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27 May 2004, BSI-PP-0010-2004
Funktionalität:	PP konform Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

SOGIS
Recognition Agreement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

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

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlussfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Common Criteria
Recognition Arrangement

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 24. Juli 2020
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

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

Matthias Intemann
Fachbereichsleiter

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Gliederung

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2. Grundlagen des Zertifizierungsverfahrens

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

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

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

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

3 Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht.
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

3. Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart.

3.1. Europäische Anerkennung von CC – Zertifikaten (SOGIS-MRA)

Das SOGIS-Anerkennungsabkommen (SOGIS-MRA) Version 3 ist im April 2010 in Kraft getreten. Es legt die Anerkennung von Zertifikaten für IT-Produkte auf einer Basisanerkennungsstufe und zusätzlich für IT-Produkte aus bestimmten Technischen Bereichen (SOGIS Technical Domain) auf höheren Anerkennungsstufen fest.

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

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

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

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

3.2. Internationale Anerkennung von CC - Zertifikaten

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

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

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den jeweiligen Stellen der Unterzeichnerstaaten als gleichwertig

anerkannt wird. Ein Hinweis unter dem Logo weist auf einen spezifischen Umfang der Anerkennung hin.

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

4. Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt c-secure-ident, Version 2.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts c-secure-ident, Version 2.0 wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz GmbH durchgeführt. Die Evaluierung wurde am 26. Juni 2020 abgeschlossen. Das Prüflabor Deutsches Forschungszentrum für Künstliche Intelligenz GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[4].

Der Sponsor und Antragsteller ist: c-trace GmbH.

Das Produkt wurde entwickelt von: c-trace GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5. Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes. Das Produkt ist unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den CC entnommen werden. Detaillierte Referenzen sind in Teil C dieses Reportes aufgelistet.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

[4] Information Technology Security Evaluation Facility

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 24. Juli 2020, ist gültig bis zum 23. Juli 2025. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

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

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

6. Veröffentlichung

Das Produkt c-secure-ident, Version 2.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[5]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[5] c-trace GmbH
Stieghorster Straße 112
33605 Bielefeld

B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1. Zusammenfassung

Der Evaluierungsgegenstand (EVG) c-secure-ident, Version 2.0 ist ein Abfallbehälter-Identifikationssystem. Er wird im Bereich der Abfallentsorgung eingesetzt, wo Abrechnungssysteme gefordert werden, die eine verursacherbezogene Gebührenabrechnung über die Anzahl der Leerungen und dadurch eine verursacherbezogene Abrechnung der Abfallgebühren zu ermöglichen.

Der EVG erfasst mit RFID-Transpondern (ID-Tag) ausgerüstete Abfallbehälter und bietet Schutz vor Datenverlust und rein zufälliger Datenverfälschung während der Speicherung im ID-Tag und im Abfallsammelfahrzeug, sowie während der Übertragung vom ID-Tag zur Sicherheitsbibliothek der Fahrzeugsoftware und von der Fahrzeugsoftware zum Sicherheitsmodul der Bürosoftware.

Für die unterschiedlichsten Einsatzzwecke stehen RFID-Transponder verschiedener Typen in diversen Bauformen zur Verfügung. Die Liste der zertifizierten Transponder wird mit dem EVG ausgeliefert.

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

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [8].

Die Vertrauenswürdigkeitskomponenten (Security Assurance Requirements SAR) sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 6 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als CC Teil 2 erweitert.

Die funktionalen Sicherheitsanforderungen werden durch die folgende Sicherheitsfunktionalität des EVG umgesetzt:

Sicherheitsfunktionalität des EVG	**Thema**
SF_ID_CHK	Prüfung, ob berechnete Prüfsumme aus übergebenen Identifikationsdaten (AT1) mit übergebener Prüfsumme übereinstimmt; Anhängen des Ergebnisses (gültig / ungültig) an den Leerungsdatensatz (AT)
SF_KEN	Schreiben der Kennung des angeschlossenen Fahrzeugrechners in neu angelegte Leerungsdatensätze (AT) und Leerungsdatenblöcke (AT+)
SF_CRC_AT	Anhängen einer Prüfsumme an einen Leerungsdatensatz (AT)
SF_CRC_AT+	Errechnen einer Prüfsumme über einen

Sicherheitsfunktionalität des EVG	Thema
	Leerungsdatenblock (AT+)
SF_SAFE	Zusammenstellen eines Leerungsdatenblocks (AT+) aus einer bestimmten Anzahl von Leerungsdatensätzen (AT), anschließend Speicherung zusammen mit Kennung und errechneter Prüfsumme im primären und sekundären Speicher
SF_KEN_CHK	Prüfen der Gültigkeit der Fahrzeugkennung im Leerungsdatensatz (AT) und im Leerungsdatenblock (AT+)
SF_AT_CHK_AT+_CHK	Prüfen der Integrität der aus dem Fahrzeugrechner empfangenen Daten (Leerungsdatenblock (AT+) und alle im AT+ enthaltenen Leerungsdatensätze (AT))

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6] Kapitel 7.1 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3 definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken den Kapitel 3.1, 3.2 und 3.3 dar.

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG: ID-Tags (RFID Transponder) in unterschiedlichen Typen und Bauformen, eine Funktionsbibliothek in der Fahrzeugsoftware, ein Funktionsmodul in der Bürosoftware sowie Benutzerdokumentation für die Besatzung des Abfallsammelfahrzeugs und für die Bediener der Bürosoftware. Für mehr Details siehe Kapitel 8.

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

2. Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heisst:

c-secure-ident, Version 2.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version/ Typbezeichnung	Auslieferungsart
1	SW	c-secure vehicle	2.0	Bestandteil des durch den EVG-Hersteller gelieferten Fahrzeugsystems
2	SW	c-secure office	2.0	Betrieb durch Hersteller im Rechenzentrum oder optionale Auslieferung an Nutzer
3	DOC	Übersicht der konformen Transpondertypen für c-secure ident 2 [10]	1.5	Lieferung durch EVG-Hersteller
4	DOC	Kurzanleitung c-ident [11]	2.04	Lieferung durch EVG-Hersteller
5	DOC	Bedienungsanleitung c-trace Identsystem c-ident 2 und c-ident 2 mit Waage [12]	2.08	Lieferung durch EVG-Hersteller
6	DOC	Benutzerhandbuch c-secure office 2.0 [13]	1.4	Lieferung durch EVG-Hersteller
7	HW	ID-Tag	RI-TRP-R9QL TRPGR30ATGA TRPGR30ATGB TRPGR30ATGC RI-INL-R9QM RI-TRP-0105 TRPGR30ENATGA RI-TRP-0108 TRPGR30ENATGB RI-INL-W007 EM4005, EM4105 EM4305, EM4269 EM4369, EM4469 EM4569 SIC7999 Monza 4 Monza R6-P	Lieferung durch EVG-Hersteller oder Hersteller des Tag
8	SW	Lifter Controller	1.27	Bestandteil des durch den EVG-Hersteller gelieferten Fahrzeugsystems
9	SW	c-secure controller	3.18	Teil der durch den Hersteller gelieferten Bürosoftware

Tabelle 2: Auslieferungsumfang des EVG

Die EVG-Komponenten können auf folgende Art identifiziert werden:

- Sicherheitsbibliothek c-secure vehicle und Komponente Lifter Controller: über die Anzeige ihrer Version am Touch Terminal des Fahrzeugrechners
- Sicherheitsmodul c-secure office und Modul c-secure Controller: über die Anzeige der Versionen an der clientseitigen Bürosoftware
- Übersicht über die konformen Transpondertypen, die Anleitungen sowie das Benutzerhandbuch: durch Titel und Version

Die Komponente Lifter Controller und das Modul c-secure Controller sind nicht Teil des EVG. Da der EVG jedoch nur über diese Komponenten genutzt werden kann, sind sie hier mit aufgeführt.

3. Sicherheitspolitik

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

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

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

4. Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind die folgenden Punkte relevant: Korrekte Handhabung der ID-Tags, der Einsatz vertrauenswürdigen Personals, Zugangsschutz zu den Komponenten des TOE (außer ID-Tags), regelmäßige Prüfung der Daten auf Vollständigkeit sowie die Sicherung der vom EVG erzeugten Daten. Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5. Informationen zur Architektur

Der EVG besteht aus drei materiell vollständig voneinander getrennten Teilsystemen:

- Kommerziell gebrauchsfertige ID-Tags (RFID Transponder)
- Sicherheitsbibliothek c-secure vehicle (Bestandteil der Fahrzeugsoftware)
- Sicherheitsmodul c-secure office (Bestandteil der Bürosoftware)

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

- vom ID-Tag zur Sicherheitsbibliothek c-secure vehicle (Identifikationsdaten mit CRC-Prüfsumme) und

- von der Sicherheitsbibliothek c-secure vehicle zum Sicherheitsmodul c-secure office (Leerungsdatenblöcke mit Fahrzeugkennung als Gültigkeitsmerkmal und mit CRC-Prüfsummen für Leerungsdatenblöcke und darin enthaltene Leerungsdatensätze)

Die Funktionalität jedes Teilsystems ist vollständig unabhängig von den anderen Teilsystemen. Alle Schnittstellen der Teilsysteme werden von der IT-Umgebung angesteuert. Um zu gewährleisten, dass die Ansteuerung der Schnittstellen dem vorgesehenen Zweck und der vorgesehenen Methode des Gebrauchs entspricht, sind bestimmte Komponenten der Fahrzeugsoftware und der Bürosoftware Bestandteil der evaluierten Konfiguration.

6. Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7. Testverfahren

Die unabhängigen Funktionstests wurden in den Räumlichkeiten der Prüfstelle durchgeführt. Der Entwickler hat hierzu einen voll funktionsfähigen Fahrzeugrechner in Form eines Demonstrators zur Verfügung gestellt. Die serverseitige Bürosoftware wurde vom Entwickler auf einem frisch installierten Server (Windows 2012 Server, Microsoft SQL Server 2017 Evaluation) der Prüfstelle installiert. Zusätzlich bestand auch die Möglichkeit, über das Internet das Produktivsystem beim Entwickler zu verwenden.

7.1. Testkonfiguration

Die Auswahl der getesteten ID-Tags und Aktionen von Fahrzeug- und Bürosoftware erfolgte anhand der durch die Aufrufschnittstellen der EVG-Bestandteile umgesetzten Sicherheitsfunktionalität.

Die einzige evaluierte Konfiguration des EVG wurde vom Entwickler so bereitgestellt, wie es auch im Kundenverhältnis vorgesehen ist. Sie ist in Kapitel 8 beschrieben. Weitere Konfigurationen oder für den Anwender vorgesehene Konfigurationsschritte sind nicht Bestandteil der evaluierten Konfiguration.

7.2. Unabhängige Evaluatortests

Für alle Sicherheitsfunktionen und funktionalen Sicherheitsanforderungen wurden Positiv- und Negativ-Tests entwickelt und durchgeführt. Dabei wurden alle Schnittstellen der funktionalen Spezifikation abgedeckt.

Die Stimulation dieser Schnittstellen und Beobachtung der Aktionen erfolgte grundsätzlich über geeignete Eingaben und Ausgaben an den externen Schnittstellen der Fahrzeug- und Bürosoftware. Für einige Tests wurde der Inhalte der USB-Speichermedien außerhalb des Fahrzeugrechners ausgelesen oder verändert. In allen Fällen entsprachen die tatsächlichen Testergebnisse den erwarteten Testergebnissen.

7.3. Penetrationstests

Im Rahmen der Schwachstellenanalyse wurden für den Produkttyp und die Evaluierungsstufe keine relevanten Schwachstellen gefunden. Daher war die Ausarbeitung und Durchführung von Penetrationstests im Rahmen der Evaluierung nicht notwendig.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgende Konfiguration des EVG:

Der EVG c-secure-ident, Version 2.0 besteht aus den folgenden Komponenten:

- RFID-Transponder mit Identifizierungsdaten (siehe Tabelle 2)
- Sicherheitsbibliothek „c-secure vehicle“, Version 2.0 als Bestandteil der Fahrzeugsoftware
- Sicherheitsbibliothek „c-secure office“, Version 2.0 als Serverkomponente
- Handbücher (siehe Tabelle 2)

Zur evaluierten Konfiguration gehören neben den EVG-Bestandteilen auch folgende Nicht-EVG-Bestandteile:

- Komponente Lifter Controller, Version 1.27
- Modul c-secure Controller, Version 3.18

Diese Bestandteile dürfen in der evaluierten Konfiguration nur mit den oben angegebenen Versionsnummern verwendet werden, da nur für diese Versionen getestet wurde, dass der EVG mit seinen Sicherheitsfunktionen korrekt aufgerufen wird.

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluierungsmethodologie CEM [2] wurde verwendet.

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

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

Die Evaluierung hat gezeigt:

- PP Konformität: Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27 May 2004, BSI-PP-0010-2004 [8]
- Funktionalität: PP konform
Common Criteria Teil 2 erweitert

- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 1 mit Zusatz von ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2. Ergebnis der kryptographischen Bewertung

Der EVG enthält keine kryptographischen Mechanismen. Folglich waren solche Mechanismen nicht Gegenstand der Evaluierung.

10. Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind alle Aspekte der Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken wie in den Sicherheitsvorgaben dargelegt, die nicht durch den EVG selbst, sondern durch die Einsatzumgebung erbracht werden müssen, zu berücksichtigen.

Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.

11. Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12. Definitionen

12.1. Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CEM	Common Methodology for Information Technology Security Evaluation - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report

IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
PP	Protection Profile – Schutzprofil
RFID	Radio Frequency Identification
SAR	Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
ST	Security Target - Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality - EVG-Sicherheitsfunktionalität

12.2. Glossar

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind.

Evaluationsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher.

EVG-Sicherheitsfunktionalität - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die SFR durchzusetzen.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine passive Einheit im EVG, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlass sein muss.

Sicherheitsvorgaben - Eine implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

Subjekt - Eine aktive Einheit innerhalb des EVG, die die Ausführung von Operationen auf Objekten bewirkt.

Zusatz - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

13. Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

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

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

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[6] https://www.bsi.bund.de/AIS

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

[6] Sicherheitsvorgaben BSI-DSZ-1063-2020, Version 1.14, 09 March 2020, Sicherheitsvorgaben für das c-trace Abfallbehälter-Identifikations-System c-ident, c-trace GmbH

[7] Evaluierungsbericht, Version 1.0, 05 June 2020, Evaluierung c-secure ident 2.0 Evaluation Technical Report, DFKI, (vertrauliches Dokument)

[8] Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27 May 2004, BSI-PP-0010-2004, Deutscher Städte- und Gemeindebund und Bundesamt für Sicherheit in der Informationstechnik

[9] Konfigurationsverzeichnis BSI Zertifizierung c-secure ident 2, Version 1.6, 09 March 2020, c-trace GmbH (vertrauliches Dokument)

[10] Übersicht der konformen Transpondertypen für c-secure ident 2, Version 1.5, c-trace GmbH

[11] Kurzanleitung c-ident, Version 2.04, 10 April 2018, c-trace GmbH

[12] Bedienungsanleitung c-trace Identsystem c-ident 2 und c-ident 2 mit Waage, Version 2.08, c-trace GmbH

[13] Benutzerhandbuch c-secure office 2.0, Version 1.4, 25 February 2020, c-trace GmbH

[6] speziell

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

C. Auszüge aus den Kriterien

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

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

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

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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