Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1063-V2-2025

zu

c-secure-ident, Version 2.2

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-V2-2025 (*)

Abfallbehälter-Identifikationssystem

c-secure-ident, Version 2.2

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, ASE_REQ.2
Gültig bis:	15. Oktober 2030

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), CEM:2022 ergänzt um Interpretationen des Zertifizierungsschemas unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, CC:2022 (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.

Common Criteria
Recognition Arrangement

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.

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, 16. Oktober 2025

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Fabian Hodouschek
Leiter der Zertifizierungsstelle

L.S

Sandro Amendola .
Direktor Abteilung S

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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 BSIG1 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]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- 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), CC:2022[4] [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 Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019, Bundesgesetzblatt I S. 1365

- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), CEM:2022 [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.

[4] Bekanntmachung des Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

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 2.2 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts c-secure-ident, Version 2.2 wurde von Deutsche Telekom Security GmbH durchgeführt. Die Evaluierung wurde am 30. September 2025 abgeschlossen. Das Prüflabor Deutsche Telekom Security GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

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 der Guidance aufgeführt sind werden beachtet.
- das Produkt wird in der operativen Einsatzumgebung betrieben, die 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. 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. Dabei

[5] Information Technology Security Evaluation Facility

behält sich das BSI das Recht vor das Zertifikat zurück zu ziehen, besonders wenn eine ausnutzbare Schwachstelle des zertifizierten Produktes bekannt wird.

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 16. Oktober 2025, ist gültig bis 15. Oktober 2030. 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 2.2 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden. Siehe auch auf der Website des BSI: https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Nähere Informationen sind auch über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[6]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[6] 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 Evaluationsgegenstand ist das Produkt c-secure ident, Version 2.2. Der EVG ist ein Abfallbehälter-Identifikationssystem, durch das Abfallbehälter mit einem ID-Tag (mit elektronischen Chip, dem Transponder) identifiziert werden, um feststellen zu können, wie oft der einzelne Abfallbehälter geleert worden ist.

Der EVG erfasst Abfallbehälter mithilfe der RFID-Technologie automatisch. Die Abfallbehälter werden mit einem ID-Tag zur eindeutigen Zuordnung zum Eigentümer ausgerüstet. Hierzu stehen verschiedene Transponder in diversen Bauformen zur Verfügung. Die Liste der zertifizierten Transponder wird mit dem EVG ausgeliefert.

Der EVG bietet Schutz vor Datenverlust und 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. Der EVG gewährleistet mit seiner Sicherheitsfunktionalität die Gültigkeit, Integrität und Vollständigkeit der zu schützenden Daten, jedoch nicht die Vertraulichkeit der Daten, insb. beinhaltet es keine Funktionalität zur Verschlüsselung.

Die Sicherheitsvorgaben [5] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [7].

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, ASE_REQ.2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [5] 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	Funktion, die aufgrund von übergebenen Identifikations-daten (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	Die Funktion, die in einen neu angelegten Leerungsdatensatz (AT) und einen neu angelegten Leerungsdatenblock (AT+) die Kennung des angeschlossenen Fahrzeugrechners schreibt.
SF_CRC_AT	Die Funktion, die an einen Leerungsdatensatz AT eine Prüfsumme anhängt.
SF_CRC_AT+	Die Funktion, die über einen Leerungsdatenblock AT+ eine Prüfsumme errechnet.

Sicherheitsfunktionalität des EVG	Thema
SF_SAFE	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	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	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 überein-stimmen. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheits-modul c-secure office für die korrekte Weiterverarbeitung genutzt.

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [5] Kapitel 7.1 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind den Sicherheitsvorgaben [5], Kapitel 3.1 definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3.3, 3.4 und 3.5 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 2.2

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	HW	ID-Tags (siehe auch DOC Nr. 5 in dieser Tabelle)	RI-TRP-R9QL, TRPGR30ATGA, TRPGR30ATGB, TRPGR30ATGC, RI-INL-R9QM, RI-TRP-0105, RI-TRP-0108, TRPGR30ENATGA, TRPGR30ENATGB, RI-INL-W007, EM4005, EM4105, EM4305, EM4269, EM4369, EM4469, EM4569, SIC7999, Monza 4, Monza R6-P	Bereitstellung durch c-trace oder Kunde
2	SW	c-secure-vehicle_tp3.lib	2.2	Installation durch c-trace
		c-secure-vehicle_ic2.lib	2.2	
3	SW	c-secure office	2.0	Installation durch c-trace
4	DOC	Kurzanleitung c-ident 2 [8]	2.05	Website-Download
		Bedienungsanleitung c-ident 2 [9]	2.39	
5	DOC	Übersicht der konformen Transpondertypen für c-secure ident 2 [10]	1.5	Website-Download
6	DOC	Benutzerhandbuch c-secure office [11]	1.6	Website-Download
7	SW	Lifter Controller	1.32	Bestandteil des durch den EVG-Hersteller gelieferten Fahrzeugsystems
8	SW	c-secure controller	3.18	Bestandteil des durch den EVG-Hersteller gelieferten Fahrzeugsystems

Tabelle 2: Auslieferungsumfang des EVG

2.1. Übersicht des Auslieferungsverfahrens

Der Lieferprozess ist nicht Teil der Evaluierung.

2.2. Möglichkeit der Identifizierung des EVGs durch den Anwender

Die Hardwarekomponente des EVGs kann nicht identifiziert werden, da es sich bei den Tokens um Komponenten von Drittanbietern handelt, die nicht mit der EVG-Referenz gekennzeichnet sind. Der Benutzer kann anhand des Dokuments [10] überprüfen, ob er kompatible Tokens verwendet. Die Versionsnummern der Softwarekomponenten sind im Menü sichtbar, wie in Abschnitt 16.4 von [9] und Abschnitt 4.3 von [11] beschrieben.

3. Sicherheitspolitik

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

- Berechnung und Überprüfung von Prüfsummen für Identifikationsdaten AT1,
- Schreiben von Identifikationsdaten des Fahrzeugcomputers in Leerungsdatensätze AT oder Leerungsdatenblöcke AT+,
- Schreiben von Prüfsummen in Leerungsdatensätze AT,
- Speichern von Leerungsdatenblöcken AT+ im Primär- und Sekundärspeicher,
- Überprüfen der Fahrzeug-ID in Leerungsdatensätzen AT und Leerungsdatenblöcken AT+ sowie
- Berechnung und Überprüfung von Prüfsummen für Leerungsdatensätze AT und Leerungsdatenblöcke AT+.

Somit gewährleistet der EVG die Integrität von Identifikationsdaten AT1, Leerungsdatensätzen AT und Leerungsdatenblöcken AT+, die Gültigkeit von Leerungsdatensätzen AT und Leerungsdatenblöcken AT+ und Redundanz bei Speicherung von Leerungsdatensätzen AT im Speicher.

Einzelheiten zu den oben genannten Sicherheitsrichtlinien sind in Abschnitt 7 der Sicherheitsvorgaben (ST) zu finden.

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:

- 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.“
Der Benutzer muss Abschnitt 16.3 von [9] konsultieren.

- 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.“
Der Benutzer muss Abschnitt 13.1 von [9] und 2.1.1 von [11] konsultieren.

- 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.“
Der Benutzer muss Abschnitt 2.1.1 von [11] konsultieren.

- 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.“
Der Benutzer muss Abschnitt 4.1.2 von [11] konsultieren.

- OE.Backup Datensicherung

„Es muss sichergestellt sein, dass der Benutzer (S-Trusted) in regelmäßigen Abständen Sicherheitskopien der vom EVG erzeugten Daten macht.“
Der Benutzer muss Abschnitt 2.1.3 von [11] konsultieren.

Details finden sich in den Sicherheitsvorgaben [5], 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, siehe Tabelle 2.

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

7.1. Unabhängige Evaluator Tests

Überblick:

Die unabhängigen Tests wurden unter Verwendung der Testumgebung des Entwicklers durchgeführt, die aus Hardware und Software besteht.

Da der EVG nur über eine Konfiguration verfügt, wurden alle Konfigurationen des EVGs getestet, die von der aktuellen Evaluierung abgedeckt werden sollen.

Unabhängiger Test Ansatz:

Der EVG wurde unabhängig in Bezug auf zwei spezifische Themenbereiche getestet: a) Korrekter Aufruf der EVG-Komponenten in der EVG-Umgebung und b) Korrekte redundante Speicherung der Leerungsdatenblöcke (AT+) im Sekundärspeicher.

EVG-Testkonfigurationen:

Es wird keine spezielle Konfiguration vorgenommen. Der EVG verfügt nur über eine einzige Konfiguration, und der EVG befindet sich immer in diesem Standardkonfigurationszustand.

Der getestete EVG ist “c-secure ident” und besteht aus den folgenden Komponenten:

- RFID-Tokens,
- c-secure-vehicle.lib als IC2 und TP3 Variante, Version 2.2, eingebettet in Hardware-IT-Systemen und
- c-secure-office.dll, Version 2.0.0.0, eingebettet in Software, die in der Cloud betrieben wird.

Ausgewählte Menge unabhängiger Tests, einschließlich einer kurzen Begründung:

Die unabhängigen Tests wurden so ausgewählt, dass Positivtests zeigen, dass die verschiedenen EVG-Komponenten sowohl für die IC2- als auch für die TP3-kompilierte Fahrzeugbibliothek erfolgreich zusammenarbeiten. Die Tests decken die folgenden SFRs ab: FDP_DAU.1, FRU_FLT.1, FDP_ITT.5 und FDP_SDI.1.

Urteil für die Teilaktivität:

Das Gesamtergebnis der Tests ist, dass keine Abweichungen zwischen den erwarteten und den tatsächlichen Testergebnissen festgestellt wurden.

7.2. Penetrationstests

Überblick:

Die Penetrationstests wurden teilweise unter Verwendung der Testumgebung des Entwicklers – bestehend aus Software – und teilweise unter Verwendung der Testumgebung der ITSEF – bestehend aus Software – durchgeführt.

Der EVG verfügt nur über eine Konfiguration. Diese wurde getestet.

Das Gesamtergebnis der Tests ist, dass keine Abweichungen zwischen den erwarteten und den tatsächlichen Testergebnissen festgestellt wurden; darüber hinaus war kein Angriffsszenario mit dem Angriffspotenzial „Basic“ tatsächlich erfolgreich.

Penetrationstest-Ansatz:

Der Prüfer untersuchte die Entwicklerdokumente [11] und [9], um relevante Informationen darüber zu finden, wie der EVG in einen ordnungsgemäßen und bekannten Zustand gebracht werden kann. Anschließend suchte er anhand der Dokumente zu den funktionalen Spezifikationen in den CVE-Einträgen nach potenziellen Schwachstellen. Anschließend leitete der Prüfer Angriffsszenarien ab, die alle potenziellen Schwachstellen abdecken. Für diese Szenarien erstellte der Prüfer Penetrationstests, sodass jedes Angriffsszenario durch mindestens einen relevanten Penetrationstest getestet wird.

EVG-Testkonfigurationen:

Es wird keine spezielle Konfiguration vorgenommen. Der EVG verfügt nur über eine einzige Konfiguration, und der EVG befindet sich immer in diesem Standardkonfigurationszustand.

Der getestete EVG ist “c-secure ident” und besteht aus den folgenden Komponenten:

- RFID-Tokens,
- c-secure-vehicle.lib als IC2- und TP3-Variante, Version 2.2, verfügbar als Quelltext und
- c-secure-office.dll, Version 2.0.0.0, eingebettet in Software, die in der Cloud betrieben wird.

Der EVG wird über Software-Schnittstellen der kompilierten EVG-Bibliotheken und über die in der Cloud gehostete Office-Suite getestet. Sowohl Quelltexte als auch Office-Suite sind übers Internet von der Prüfstelle aus zugänglich.

Getestete Angriffsszenarien:

- AS.1: Der EVG empfängt manipulierte AT1-Daten,
- AS.2: Der EVG empfängt manipulierte AT+-Daten,
- AS.3: Der EVG verliert Daten, die in seinem Primärspeicher gespeichert sind.

Getestete SFRs:

- FDP_ITT.5,
- FDP_SDI.1 und
- FRU_FLT.1.

Urteil für die Teilaktivität:

Das Gesamtergebnis des Tests lautet, dass keine Abweichungen zwischen den erwarteten und den tatsächlichen Testergebnissen festgestellt wurden. Kein Angriffsszenario mit dem Angriffspotenzial „Basic“ war in der in [5] definierten Betriebsumgebung des EVGs tatsächlich erfolgreich, vorausgesetzt, dass alle vom Entwickler geforderten Maßnahmen angewendet wurden.

8. Evaluierte Konfiguration

Der EVG besteht aus den folgenden Komponenten:

- ID-Tags (siehe Dokument „Übersicht der konformen Transpondertypen für c-secure ident 2“ [10] und Tabelle 2)
- Sicherheitsbibliothek c-secure-vehicle_tp3.lib und c-secure-vehicle_ic2.lib, Version 2.2 als Bestandteil der Fahrzeugsoftware. Dies sind zwei Binärversionen der gleichen Komponente, die für zwei unterschiedliche Plattformen kompiliert wurden. Im EVG kommt je nach Zielsystem lediglich eine der beiden Bibliotheken zum Einsatz.
- Sicherheitsbibliothek c-secure-office.dll, Version 2.0.0.0 als Serverkomponente
- Handbücher (siehe Tabelle 2)

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

- Komponente Lifter Controller, Version 1.32
- Modul c-secure-controller.dll, Version 3.18

Alle Versionen sind auch in Tabelle 2 aufgeführt.

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [6] 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, 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 [7]
- 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, 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 Politiken 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.

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

Auflagen für den Einsatz des evaluierten Produktes:

- Dem Benutzer wird empfohlen, vor der ersten Verwendung des EVGs die Anweisungen in Abschnitt 13 von [9] und Abschnitt 2 von [11] zu befolgen.

11. Sicherheitsvorgaben

Die Sicherheitsvorgaben [5] 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
CRC	Cyclic Redundancy Check
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
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
WBIS	Waste Bin Identification Systems (Abfallbehälter-Identifikations-System)

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.

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),
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
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
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.

[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[7] https://www.bsi.bund.de/AIS

[5] Sicherheitsvorgaben BSI-DSZ-1063-V2, Version 1.20, 30.05.2025, Sicherheitsvorgaben für das c-trace Abfallbehälter-Identifikations-System c-ident, c-trace GmbH

[6] Evaluierungsbericht, Version 1.2, 01.09.2025, Common Criteria Single Evaluation Report ETR Summary, Deutsche Telekom Security GmbH (vertrauliches Dokument)

[7] specifically

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

[7] Protection Profile Waste Bin Identification Systems (WBIS-PP), Version 1.04, 27.05.2004, BSI-PP-0010-2004, Deutscher Städte- und Gemeindebund und Bundesamt für Sicherheit in der Informationstechnik

[8] Kurzanleitung c-ident 2, c-trace GmbH, Version 2.05, 04.05.2020

[9] Bedienungsanleitung c-trace Identsystem c-ident 2 und c-ident 2 mit Waage, c-trace GmbH, Version 2.39, 07.05.2025

[10] Übersicht der konformen Transpondertypen für c-secure ident 2, c-trace GmbH, Version 1.5, 09.03.2020

[11] Benutzerhandbuch c-secure office 2.0.0.0, c-trace GmbH, Version 1.6, 15.05.2025

[12] Konfigurationsverzeichnis BSI Zertifizierung c-secure ident 2, c-trace GmbH, Version 1.12, 30.05.2025

C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC:2022 können dazu genutzt werden:

- Definition und Beschreibung zu Conformance Claims: CC:2022 Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -kompomenten: CC:2022 Teil 3 Kapitel 6.1,
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 5,
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC:2022 Teil 3 Kapitel 9,
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC:2022 Teil 3 Kapitel 7 bis 15,
- Die Tabelle 1 in CC:2022 Teil 5, Kapitel 4.2 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.

Bemerkung: Ende des Reportes