Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1013-2017

zu

IMELO-Secure, Version 1.0

der

Institut für Entsorgung und Umwelttechnik 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-1013-2017 (*)

Abfallbehälter-Identifikationssystem

IMELO-Secure
Version 1.0

von	Institut für Entsorgung und Umwelttechnik 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_OBJ.2, ASE_REQ.2, ASE_SPD.1

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement

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. 4 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.

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. August 2017

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Joachim Weber
Fachbereichsleiter

L.S.

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

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.

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.

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

Gliederung

A. Zertifizierung

1. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[2]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[3]
- BSI-Kostenverordnung[4]
- 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[5] [1], auch als Norm ISO/IEC 15408 veröffentlicht.
- 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]

2. 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.

2.1. Europäische Anerkennung von ITSEC/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

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

[3] 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

[4] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

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

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 EAL1 bis EAL4 und ITSEC Vertrauenswürdigkeitsstufen E1 bis E3 (niedrig) 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.

Das Abkommen wurde von den nationalen Stellen von Deutschland, Finnland, Frankreich, Großbritannien, Italien, Niederlande, Norwegen, Österreich, Schweden und Spanien unterzeichnet. Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

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

2.2. Internationale Anerkennung von CC - Zertifikaten

Das internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf den Common Criteria (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).

Das CCRA-2014 ersetzt das frühere CCRA, das im Mai 2000 unterzeichnet worden war (CCRA-2000). CC-Zertifikate, die vor dem 8. September 2014 nach den Regelungen des CCRA-2000 erteilt wurden, fallen weiterhin unter die gegenseitige Anerkennung. Für Zertifizierungsverfahren, die am 8. September 2014 bereits angefangen hatten, sowie für Verfahren zur Aufrechterhaltung alter Zertifikate (Maintenance and Re-Zertifizierungen) wurde eine Übergangsfrist zur Anerkennung nach den Regelungen des CCRA-2000 bis bis 8. September 2017 vereinbart (d.h. für Vertrauenswürdigkeitsstufen bis einschließlich EAL 4 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR).

Im September 2014 wurde das Abkommen CCRA-2014 von den nationalen Stellen von Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn und USA unterzeichnet.

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

Das CCRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens von den oben genannten Nationen anerkannt wird.

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

3. 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 IMELO-Secure, Version 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts IMELO-Secure, Version 1.0 wurde von der TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 11. August 2017 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor und Antragsteller ist: Institut für Entsorgung und Umwelttechnik GmbH.

Das Produkt wurde entwickelt von: Institut für Entsorgung und Umwelttechnik GmbH.

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

4. Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes.

Das Produkt ist nur 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 Vertrauenswürdigkeitsstufen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports und in den CC selbst erläutert.

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 Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den

[6] Information Technology Security Evaluation Facility

Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 16. August 2017, ist gültig bis 15. August 2022. 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 den Hersteller 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.

5. Veröffentlichung

Das Produkt IMELO-Secure, Version 1.0 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[7]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[7] Institut für Entsorgung und Umwelttechnik GmbH

Kalkofen 6
58638 Iserlohn

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) wird als IMELO-Secure, Version 1.0 bezeichnet und ist ein Abfallbehälter-Identifikationssystem, das aus den folgenden Komponenten besteht:

- ID-Tag (LF- oder UHF-Transponder),
- Sicherheitsmodul IMELO-Secure.dll V1.0
  in der Fahrzeugsoftware und in der Bürosoftware
- Handbücher.

Abfallbehälter-Identifikationssysteme (WBIS) im Sinne des zugrundeliegenden Protection Profiles 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 Identifizierung von Abfällen, sondern um die Identifizierung der Behälter, in denen Abfälle zur Entsorgung bereitgestellt werden.

Die Abfallbehälter werden mit einem Transponder (ID-Tag) ausgestattet. Der ID-Tag speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Identifizierungsdatensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Leser ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle zufällige Manipulationen werden vom Sicherheitsmodul der Fahrzeugsoftware erkannt.

Das Sicherheitsmodul der Fahrzeugsoftware ergänzt diese Identifizierungsdaten um Datum- und Zeitangaben, bildet daraus einen Leerungsdatensatz AT und speichert diesen CRC-geschützt auf dem Fahrzeugrechner. Die Leerungsdatensätze AT werden vom Sicherheitsmodul in Leerungsdatenblöcken AT+ zusammengefasst, die Leerungsdatenblöcke AT+ um eine Gültigkeitskennung ergänzt und durch CRC-Checksummen integritätsgeschützt an die Bürosoftware übermittelt. Das Sicherheitsmodul in der Fahrzeugsoftware sorgt durch geeignete Maßnahmen (z.B. Backup der Daten) dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist.

Nach der Übermittlung der Leerungsdatenblöcke AT+ an die Bürosoftware wird durch das Sicherheitsmodul der Bürosoftware sichergestellt, dass nur die in einem registrierten Fahrzeug erstellten Leerungsdatenblöcke AT+ als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler oder zufälligen Manipulationen erkannt.

Nach der Prüfung der übertragenen Daten durch das Sicherheitsmodul können diese Daten an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

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_OBJ.2, ASE_REQ.2, ASE_SPD.1.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 5.1 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 folgenden Sicherheitsfunktionen des EVG umgesetzt:

Sicherheitsfunktionen des EVG	Thema
SF_ID_CHECK_LF	Integritätsprüfung von LF-Transponder-IDs
SF_ID_CHECK_UHF	Integritätsprüfung von UHF-Transponder-IDs
SF_CRC_GEN_AT	Generierung und Integritätssicherung eines Leerungsdatensatzes AT
SF_CRC_GEN_ATP	Generierung und Integritäts- sowie Gültigkeitssicherung eines Leerungsdatenblocks AT+
SF_CRC_CHECK_AT	Integritätsprüfung von Leerungsdatensätzen AT
SF_CRC_CHECK_ATP	Integritätsprüfung von Leerungsdatenblöcken AT+
SF_MID_CHECK	Gültigkeitsprüfung von Leerungsdatenblöcken AT+
SF_STORE_ATP	Redundantes Speichern von Leerungsdatenblöcken AT+
SF_RESTORE_ATP	Auslesen von Leerungsdatenblöcken AT+

Tabelle 1: Sicherheitsfunktionen des EVG

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

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

Dieses Zertifikat umfasst die folgenden Konfigurationen des EVG: Abhängig von der Transponder-Technologie werden zwei Konfigurationen des EVG identifiziert: eine mit LF-Transpondern und eine mit UHF-Transpondern. Die EVG-Software IMELO-Secure.dll und die Handbücher sind für beide Konfigurationen identisch. 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:

IMELO-Secure, Version 1.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr.	Typ	Bezeichnung	Artikelnummer/Version	Auslieferungsart
EVG-Bestandteile				
1	HW	LF-Transponder gemäß DIN30745 [13]	2021273, 2021274, 1150626, 1150627, 1150630, 1150638, 1150642, 1150648, 1150652	Die Transponder werden durch den Hersteller an den Kunden ausgeliefert.
2	HW	UHF-Transponder gemäß DIN30745 [13]	1151006, 1151007, 1151008, 1151009, 1150658	Die Transponder werden durch den Hersteller an den Kunden ausgeliefert.
3	SW	Sicherheitsmodul der Fahrzeug-Software IMELO-Secure.dll	1.0 SHA-256-Prüfsumme: 9f0c0418b7fc3607c5f8c63ca1b2a145caf6c69d1b15cceba406e757e6fb4a2f	Auf dem Fahrzeugrechner durch den Hersteller vorinstalliert und konfiguriert.
4	SW	Sicherheitsmodul der Büro-Software IMELO-Secure.dll	1.0 SHA-256-Prüfsumme: 9f0c0418b7fc3607c5f8c63ca1b2a145caf6c69d1b15cceba406e757e6fb4a2f	Download von der Herstellerseite oder Installation durch den Hersteller.
5	DOK	IMELO-Ident Ergänzendes Benutzerhandbuch zur Handhabung der Sicherheitsfunktionen nach Common Criteria für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0 [10]	V4, 2017-06-01	Email
6	DOK	IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO FTP-Importdienst Installationsanleitung für das Behälter-Identifikationssystem „IMELO-Secure“ Version 1.0 [11]	V3, 2017-06-01	Email
7	DOK	IMELO-Ident Fahrzeugsoftware Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0 [12]	V3, 2017-06-01	Email

Nr.	Typ	Bezeichnung	Artikelnummer/Version	Auslieferungsart
Nicht-EVG-Bestandteile				
8	HW	Fahrzeugrechner Variante 1: Lüfterloser Truck-PC für erweiterten Temperaturbereich unter Windows XP, Windows 7 oder höher mit GPS-, UMTS/LTE-Modul, RS485-, RS232-Schnittstelle, Digital I/O, USB und CAN-Schnittstelle.	-	Durch den Hersteller vorinstalliert und konfiguriert.
9	HW	Fahrzeugrechner Variante 2: Mobiler Fahrzeugrechner unter Windows 7 oder höher mit GPS, UMTS/HSDPA-Modul, Farbkamera, USBSchnittstelle zu CarCradle mit RS485- , RS232-Schnittstelle, Digital I/O und CAN-Schnittstelle.	-	Durch den Hersteller vorinstalliert und konfiguriert.
10	SW	Fahrzeugrechner Software	Windows Desktop-Applikation IMELO-i2 mit den Modulen, die die IMELO-Secure.dll aufrufen: ● i2Ident V1.2.x ● i2Prozess V3.2.x ● i2Transfer V3.2.x	Durch den Hersteller vorinstalliert und konfiguriert.
11	SW	Bürorechner Software	Windows Desktop-Applikation IMELODispo2 mit dem Modul, das die IMELO-Secure.dll aufruft: ● Ifeu.ImeloDispo2.FtpImport Dienst.exe V1.2.x	Download von der Herstellerseite oder Installation durch den Hersteller

Tabelle 2: Auslieferungsumfang

Da die gewählte Evaluierungsstufe EAL1+ die Vertrauenswürdigkeitskomponente ALC_DEL.1 nicht enthält, wurde die Sicherheit bei der Auslieferung nicht evaluiert.

Die Transponder werden durch den Hersteller an den Kunden ausgeliefert. Der Kunde prüft die Artikelnummer auf der Verpackung der gelieferten Transponder und vergleicht diese mit der Liste der zulässigen Transponder in den Sicherheitsvorgaben [6], Kapitel 9.1 oder in der obigen Tabelle.

Die Installation der Fahrzeugsoftware wird ausschließlich durch IMELO-Techniker vorgenommen. Der Kunde erhält einen fertig konfigurierten Fahrzeugrechner. Die Integrität des Sicherheitsmoduls in der Fahrzeugsoftware kann durch die SHA-256 Prüfsumme des Moduls, die in obiger Tabelle angegeben ist, überprüft werden. Nähere Informationen sind im Handbuch [12], Kapitel 2.4 dargestellt. Wenn das Ergebnis dieser Berechnung nicht mit oben angegebenem Wert übereinstimmt, konnte die Integrität nicht verifiziert werden und der Kundendienst des Herstellers sollte kontaktiert werden.

Die Installation der Bürosoftware wird entweder durch den Systemadministrator des Kunden oder durch Techniker des Herstellers gemäß Handbuch vorgenommen. Die Integrität des Sicherheitsmoduls in der Bürosoftware kann durch die SHA-256 Prüfsumme des Moduls, die in obiger Tabelle angegeben ist, überprüft werden. Hierzu muss für die Datei „IMELO-Secure.dll“, welche sich im Installationsverzeichnis von IMELO Dispo2 befindet, das während des Installationsvorgangs festgelegt wurde, der SHA-256 Hashwert

berechnet werden. Nähere Informationen sind im Handbuch [11], Kapitel 2.4 dargestellt. Wenn das Ergebnis dieser Berechnung nicht mit oben angegebenem Wert übereinstimmt, konnte die Integrität nicht verifiziert werden und der Kundendienst des Herstellers sollte kontaktiert werden.

Die Adressaten der Handbücher erhalten diese in digitaler Form per E-Mail. Der Disponent ist für die Weitergabe des Benutzerhandbuches an die Fahrzeugbesatzung verantwortlich.

3. Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte: Integritätsprüfung von LF-Transponder-IDs, Integritätsprüfung von UHF-Transponder-IDs, Generierung und Integritätssicherung eines Leerungsdatensatzes AT, Generierung und Integritäts- sowie Gültigkeitssicherung eines Leerungsdatenblocks AT+, Integritätsprüfung von Leerungsdatensätzen AT, Integritätsprüfung von Leerungsdaten-blöcken AT+, Gültigkeitsprüfung von Leerungsdatenblöcken AT+, Redundantes Speichern von Leerungsdatenblöcken AT+, Auslesen von Leerungsdatenblöcken AT+.
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: An den Abfallbehältern fest verbaute Transponder mit eindeutigen IDs, vertrauenswürdiges Personal, wirksamer Zugangsschutz zu SW-Bestandteilen des TOE, Überprüfung der Vollständigkeit der übertragenen Daten, Datensicherung in der Büro-Einsatzumgebung und eindeutige Mobilgerätekennungen.
Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5. Informationen zur Architektur

Der EVG ist ein verteiltes System.
Er besteht aus den Transpondern (ID-Tags), die an den Abfallbehältern befestigt sind. Sie beinhalten die eindeutige ID, gesichert durch eine CRC-16-Prüfsumme.
Des Weiteren besteht er aus dem Sicherheitsmodul IMELO-Secure.dll, V1.0, welches von der Fahrzeugsoftware (Windows Desktop-Applikation IMELO-i2 mit den Modulen i2Ident V1.2.x, i2Prozess V3.2.x, i2Transfer V3.2.x) bzw. der Bürosoftware (Windows Desktop-Applikation IMELO-Dispo2 mit dem Modul Ifeu.ImeloDispo2.FtpImportDienst.exe V1.2.x) aufgerufen wird, um die Sicherheitsfunktionalität auf dem Fahrzeug und dem Bürorechner zu erbringen.

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. Testkonfiguration

Die Tests wurden in der Prüfstelle mit einer Testumgebung, die durch den Hersteller bereitgestellt wurde, durchgeführt. Sie umfasst:

- einen Standard-LF-Leser (134,2 kHz nach DIN30745 [13]),
- einen Standard-UHF-Leser (868 MHz nach DIN30745 [13]),
- einen konfigurierten Fahrzeugrechner mit UMTS-Modul und Touchscreen,
- ein Standard-Büronotebook,
- Testsoftware des Herstellers.

Der EVG besteht aus dem Sicherheitsmodul IMELO-Secure.dll V1.0 für den Fahrzeug- und Bürocomputer und LF- sowie UHF-Transpondern, wie in den Sicherheitsvorgaben [6], Kapitel 9.1 aufgelistet. Alle der aufgelisteten Transponder wurden getestet. Es wurden jedoch nicht alle Tests mit jedem Transponder durchgeführt.

7.2. Unabhängige Evaluatortests

Es wurden alle in der funktionalen Spezifikation dokumentierten TSF-Schnittstellen getestet, wodurch alle EVG Sicherheitsfunktionalitäten durch Tests abgedeckt wurden.

Die Testdokumentation und die Testprotokolle beinhalten Details und Anmerkungen zur Testkonfiguration, dem verwendeten Testequipment, der Testprozedur und den erwarteten Ergebnissen. Die Testvoraussetzungen, Testschritte und erwarteten Ergebnisse testen die jeweilige Schnittstelle auf angemessene Weise und sind konsistent zur Beschreibung der Schnittstelle in der funktionalen Spezifikation.

Während der Prüfstellentests verhielt sich der EVG wie spezifiziert. Es gab keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen.

7.3. Penetrationstests

In der Schwachstellenanalyse wurden zwei Angriffsszenarien identifiziert, die potentiell in der angenommenen Einsatzumgebung des EVG ausnutzbar sein könnten:

- Zufällige Manipulation der Transponder-ID im Speicher des Transponders oder während des Auslesens
- Zufällige Manipulation der Leerungsdatensätze oder -blöcke während der Verarbeitung und des Speicherns auf dem Fahrzeugrechner oder während des Datentransfers zum Bürorechner

Die Penetrationstests haben gezeigt, dass sich der EVG wie erwartet verhält und diese Angriffsszenarien nicht ausnutzbar sind.

Mit der Durchführung der Schwachstellenanalyse wurde festgestellt, dass der EVG frei von Schwachstellen ist, welche durch einen Angreifer mit dem Angriffspotenzial Basic ausnutzbar sind.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

Der EVG IMELO-Secure, Version 1.0 besteht aus den folgenden Komponenten:

- LF- oder UHF-Transponder mit Identifizierungsdaten (siehe Tabelle 2)
- Modul IMELO-Secure.dll V1.0 in der Fahrzeugsoftware und in der Bürosoftware
- Handbücher (siehe Tabelle 2)

Die Sicherheitsvorgaben identifizieren abhängig von der Transponder-Technologie zwei Konfigurationen des EVG: Eine mit LF-Transpondern und eine mit UHF-Transpondern. Das Sicherheitsmodul IMELO-Secure.dll und die Handbücher sind für beide Konfigurationen identisch.

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

- Fahrzeugrechner-Software: Windows Desktop-Applikation IMELO-i2 mit den Modulen i2Ident V1.2.x[8], i2Prozess V3.2.x, i2Transfer V3.2.x
- Bürorechner-Software: Windows Desktop-Applikation IMELO-Dispo2 mit dem Modul Ifeu.ImeloDispo2.FtpImportDienst.exe V1.2.x

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 Vertrauenswürdigkeits-komponenten bestätigt:

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

[8]Produktänderungen, die eine Änderung der dritten Stelle der Versionsnummer zur Folge haben, haben keinen Einfluss auf die Sicherheitsfunktionalität des EVG und sind somit nicht relevant für die evaluierte Konfiguration. Daher trägt die dritte Stelle der Versionsnummer in diesem Zertifizierungsreport ein „x“.

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_OBJ.2, ASE_REQ.2, ASE_SPD.1

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.

Zertifizierte Aktualisierungen des EVG, die die Vertrauenswürdigkeit betreffen, sollten verwendet werden, sofern sie zur Verfügung stehen. Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen. In der Zwischenzeit sollte der Risikomanagementprozess für das IT-System, in dem der EVG eingesetzt wird, prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müssen, um die Systemsicherheit aufrecht zu erhalten.

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
CRC	Cyclic Redundancy Code
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
IFEU GmbH	Institut für Entsorgung und Umwelttechnik GmbH
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
LF	Low Frequency
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
SHA	Secure Hash Algorithm
ST	Security Target - Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
UHF	Ultra High Frequency
WBIS	Waste Bin Identification System – Abfallbehälter-Identifikationssystem

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 Sicherheits-anforderungen 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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://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. 4, September 2012, http://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[9] 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-1013-2017, Version 3, 2017-05-05, IMELO-Ident Sicherheitsvorgabe für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0, IFEU GmbH

[7] Evaluierungsbericht, Version 3, 2017-08-10, TÜV Informationstechnik GmbH (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] Konfigurationsliste für den EVG, Version 2, 2017-06-02, IMELO-Ident Versionskonzept und Konfigurationsliste für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0, IFEU GmbH (vertrauliches Dokument)

[10] IMELO-Ident Ergänzendes Benutzerhandbuch zur Handhabung der Sicherheitsfunktionen nach Common Criteria für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0, V4, 2017-06-01, IFEU GmbH

[11] IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO FTP-Importdienst Installationsanleitung für das Behälter-Identifikationssystem „IMELO-Secure“ Version 1.0, V3, 2017-06-01, IFEU GmbH

[12] IMELO-Ident Fahrzeugsoftware Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.0, V3, 2017-06-01, IFEU GmbH

[13] DIN 30745:2014-06: Elektronische Identifikation von Abfallsammelbehältern durch Transpondertechnologie mit Frequenzen unter 135 kHz und 868 kHz

[9] speziell

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

C. Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 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 EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Dies ist eine eingefügte Leerseite.