Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1013-V2-2022

zu

IMELO-Secure, Version 1.1

der

SSI Schäfer Plastics 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-V2-2022 (*)

Abfallbehälter-Identifikationssystem

IMELO-Secure
Version 1.1

von	SSI Schäfer Plastics 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 konform
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 1 mit Zusatz von ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2

SOGIS
Recognition Agreement

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

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

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, 14. Dezember 2022

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Sandro Amendola
Abteilungspräsident

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.

Gliederung

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG 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 und für Heimat
- 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[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), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

3. Anerkennungsvereinbarungen

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

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

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

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

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

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

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

3.2. Internationale Anerkennung von CC - Zertifikaten

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

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

[4] Bekanntmachung des Bundesministeriums des Innern und für Heimat vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

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 IMELO-Secure, Version 1.1 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-1013-2017. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-1013-2017 wiederverwendet.

Die Evaluation des Produkts IMELO-Secure, Version 1.1 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 5. Dezember 2022 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller ist: SSI Schäfer Plastics GmbH.

Das Produkt wurde entwickelt von: SSI Schäfer Plastics GmbH.

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

5. Gültigkeit des Zertifizierungsergebnisses

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

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

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

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

[5] Information Technology Security Evaluation Facility

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 Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 14. Dezember 2022, ist gültig bis 13. Dezember 2027. 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 IMELO-Secure, Version 1.1 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[6]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[6] SSI Schäfer Plastics GmbH
Kalkofen 6
58638 Iserlohn
Deutschland

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 1.1 bezeichnet und ist ein Abfallbehälter-Identifikationssystem, das aus den folgenden Komponenten besteht:

- ID-Tag (LF- oder UHF-Transponder),
- Sicherheitsmodul IMELO-Secure.dll V1.1
  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_SPD.1, ASE_REQ.2, ASE_OBJ.2.

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 folgende Sicherheitsfunktionalität des EVG umgesetzt:

Sicherheitsfunktionalität 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+
SF_MID_CHECK_AT	Gültigkeitsprüfung von Leerungsdatensätzen AT

Tabelle 1: Sicherheitsfunktionalität des EVG

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

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken 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 1.1

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Artikelnummer/Version	Auslieferungsart
EVG-Bestandteile				
1	HW	LF-Transponder gemäß DIN30745 [13]	2021273, 2021274, 1150626, 1150627, 1150630, 1150638, 1150642, 1150648, 1150652, 1151050	Die Transponder werden durch den Hersteller an den Kunden ausgeliefert.
2	HW	UHF-Transponder gemäß DIN30745 [13]	1151007, 1151008, 1150658, 1151009, 1150688, 1150696, 1150700, 1150702	Die Transponder werden durch den Hersteller an den Kunden ausgeliefert.
3	SW	Sicherheitsmodul der Fahrzeugsoftware	V1.1, SHA-256 Prüfsumme: e56f88d08836ffd8b0c356eadaa14f3c3fed9cb27b4fbdc9a93686dffde1a8e7	Durch den Hersteller vorinstalliert und konfiguriert.
4	SW	Sicherheitsmodul der Bürosoftware	V1.1, SHA-256 Prüfsumme: e56f88d08836ffd8b0c356eadaa14f3c3fed9cb27b4fbdc9a93686dffde1a8e7	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 1.1	V6, 2022-07-07	Email
6	Dok	IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO FTP-Importdienst Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1	V7, 2022-07-12	Email
7	Dok	IMELO-Ident Fahrzeugsoftware Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1	V5, 2022-07-07	Email
Nicht-EVG-Bestandteile				
8	HW	Fahrzeugrechner Variante 1 Lüfterloser Truck-PC für erweiterten Temperaturbereich unter Windows XP, Windows 7, Windows 10 oder höher mit GPS-, UMTS/LTE-Modul, RS485-, RS232-Schnittstelle, Digital I/O, USB und CAN-Schnittstelle.	-	Durch den Hersteller vorinstalliert und konfiguriert.

Nr	Typ	Identifier	Artikelnummer/Version	Auslieferungsart
9	HW	Fahrzeugrechner Variante 2 Mobiler Fahrzeugrechner unter Windows 7, Windows 10 oder höher mit GPS, UMTS/HSDPA-Modul, Farbkamera, USB-Schnittstelle zu CarCradle mit RS485-, RS232-Schnittstelle, Digital I/O und CAN-Schnittstelle.	-	Durch den Hersteller vorinstalliert und konfiguriert.
10	SW	Software Fahrzeugrechner	Windows Desktop-Applikation IMELO-i2 mit den Modulen, die die IMELO-Secure.dll aufrufen: i2Ident V1.2.x , i2Prozess V3.2.x, i2Transfer V3.3.x	Durch den Hersteller vorinstalliert und konfiguriert.
11	SW	Software Bürorechner	Windows Desktop-Applikation IMELODispo2 mit den Modulen, die die IMELO-Secure.dll aufruft: Ifeu.ImeloDispo2.Import.dll V1.3.x Ifeu.ImeloDispo2.Tourmonitor .dll V1.0.x	Download von der Herstellerseite oder Installation durch den Hersteller

Tabelle 2: Auslieferungsumfang des EVG

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 Integritäts- sowie Gültigkeitssicherung eines Leerungsdatensatzes AT, Generierung und Integritäts- sowie Gültigkeitssicherung eines Leerungsdatenblocks AT+, Integritätsprüfung von Leerungsdatensätzen AT und Leerungsdatenblöcken AT+, Gültigkeitsprüfung von Leerungsdatensätzen AT und Leerungsdatenblöcken AT+, Redundantes Speichern von Leerungsdatenblöcken AT+, Auslesen von Leerungsdatenblöcken AT+.

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6 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, V1.1, welches von der Fahrzeugsoftware (Windows Desktop-Applikation IMELO-i2 mit den Modulen i2Ident V1.2.x, i2Prozess V3.2.x, i2Transfer V3.3.x) bzw. der Bürosoftware (Windows Desktop-Applikation IMELODispo2 mit den Modulen Ifeu.ImeloDispo2.Import.dll V1.3.x und Ifeu.ImeloDispo2.Tourmonitor.dll V1.0.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]),
- einen Standard-UHF-Leser (868 MHz nach [DIN30745]),
- einen konfigurierten Fahrzeugrechner (Windows 10) mit UMTS-Modul und Touchscreen,
- ein Standard-Büronotebook (Windows 10) und
- Testsoftware des Herstellers.

Der EVG besteht aus dem Sicherheitsmodul IMELO-Secure.dll V1.1 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 1.1 besteht aus den folgenden Komponenten:

- LF- oder UHF-Transponder mit Identifizierungsdaten (siehe Tabelle 2)
- Sicherheitsmodul IMELO-Secure.dll V1.1 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[7], i2Prozess V3.2.x, i2Transfer V3.3.x
- Bürorechner-Software: Windows Desktop-Applikation IMELO-Dispo2 mit den Modulen Ifeu.ImeloDispo2.Import.dll V1.3.x und Ifeu.ImeloDispo2.Tourmonitor.dll V1.0.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_SPD.1, ASE_REQ.2, ASE_OBJ.2

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-1013-2017 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-

[7]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“.

Evaluierung konzentrierte sich insbesondere auf hinzugefügte Transponder und Änderungen an Hardware- und Software-Komponenten in der EVG-Umgebung.

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

CRC Cyclic Redundancy Code

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

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

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 Sicherheitsanforderungen für eine Kategorie von EVG.

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

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

13. Literaturangaben

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

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

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

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[8] 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] IMELO-Ident Sicherheitsvorgabe für das Behälter Identifikationssystem „IMELOSecure“ Version 1.1, Version 9, 14. September 2022, SSI Schäfer Plastics GmbH

[7] Evaluierungsbericht, Version 4, 28. Oktober 2022, 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] IMELO-Ident Versionskonzept und Konfigurationsliste für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1, Version 8, 14.09.2022, SSI Schäfer Plastics GmbH (vertrauliches Dokument)

[10] IMELO-Ident Ergänzendes Benutzerhandbuch zur Handhabung der Sicherheitsfunktionen nach Common Criteria für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1, Version 6, 07.07.2022, SSI Schäfer Plastics GmbH

[11] IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO FTP-Importdienst Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1, Version 7, 12.07.2022, SSI Schäfer Plastics GmbH

[12] IMELO-Ident Fahrzeugsoftware Installationsanleitung für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1, Version 5, 07.07.2022, SSI Schäfer Plastics GmbH

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

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

C. Auszüge aus den Kriterien

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

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

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

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Bemerkung: Ende des Reportes