Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0689-V2-2018

zu

CARD STAR /memo3,
FW-Version 4.0.6, HW-Versionen B00/B01

der

CCV Deutschland 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-0689-V2-2018 (*)

eHealth: Smart Card Readers

CARD STAR /memo3
FW-Version 4.0.6, HW-Versionen B00/B01

von	CCV Deutschland GmbH
PP-Konformität:	Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 19 January 2015
Funktionalität:	PP konform Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 und AVA_VAN.5

SOGIS
Recognition Agreement
für Komponenten bis
EAL 4

Common Criteria

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

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

Common Criteria
Recognition Arrangement
Anerkennung nur für
Komponenten bis EAL 2

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, 25. Juni 2018

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Bernd Kowalski L.S.
Abteilungspräsident

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

Dies ist eine eingefügte Leerseite.

A. Zertifizierung

1. Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG1 die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

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

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

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

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

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

2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- BSI-Kostenverordnung[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]

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

- 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.
- 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 EAL1 bis EAL4 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 http://www.sogisportal.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 unter die Anerkennung nach den Regeln des SOGIS-MRA, d.h. bis einschließlich der Komponenten nach CC Teil 3 EAL 4. Die Evaluierung beinhaltete die Komponente AVA_VAN.5, die nicht nach den Regelungen des SOGIS-MRA anerkannt ist. Für die Anerkennung ist hier die EAL 4 Komponente AVA_VAN.3 maßgeblich.

3.2. Internationale Anerkennung von CC - Zertifikaten

Da internationale Abkommen zur gegenseitigen Anerkennung von Zertifikaten basierend auf CC (Common Criteria Recognition Arrangement, CCRA-2014) wurde am 8. September 2014 ratifiiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis

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

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 http://www.commoncriteriaportal.org eingesehen werden.

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

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014, d.h. Anerkennung bis einschließlich CC Teil 3 EAL 2 Komponenten.

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 CARD STAR /memo3, FW-Version 4.0.6, HW-Versionen B00/B01 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts CARD STAR /memo3, FW-Version 4.0.6, HW-Versionen B00/B01 wurde von datenschutz cert GmbH durchgeführt. Die Evaluierung wurde am 5. Juni 2018 abgeschlossen. Das Prüflabor datenschutz cert GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Antragsteller ist: CCV Deutschland GmbH.

Das Produkt wurde entwickelt von: CCV Deutschland 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

[5] Information Technology Security Evaluation Facility

Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

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 25. Juni 2018, ist gültig bis 24. Juni 2023 . 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 CARD STAR /memo3, FW-Version 4.0.6, HW-Versionen B00/B01 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] CCV Deutschland GmbH
Helmholzstraße 2-9
10587 Berlin

Dies ist eine eingefügte Leerseite.

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) ist das mobile Kartenterminal CARD STAR /memo3, Firmware Version 4.0.6, Hardware Versionen B00 und B01 des Herstellers CCV Deutschland GmbH, Celectronic eHealth Division. Der EVG hat zwei integrierte Kartenleser für Smartcards und ist für den mobilen Einsatz durch medizinisches Personal vorgesehen, um Versichertendaten aus einer elektronischen Gesundheitskarte, die im deutschen Gesundheitswesen genutzt wird, auszulesen.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile [9].

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 3 mit Zusatz von ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 und AVA_VAN.5.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6.1 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.DATEN	Schutz der Daten
SF.ANZEIGE	Sichere Anzeige von Notfalldaten
SF.I&A	Identifizierung & Authentifizierung
SF.KARTEN	Kartenkommunikation
SF.MANAGE	Management
SF.DMS	Kommunikation mit dem Hostsystem
SF.TESTS	Selbsttests
Darüber hinaus verfügt der EVG über folgende Sicherheitsmaßnahme:	
SM.SIEGEL	Versiegelung

Tabelle 1: Sicherheitsfunktionalität des EVG

Mehr Details sind in den Sicherheitsvorgaben [6] Kapitel 7 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 1.4.8, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

Dieses Zertifikat umfasst die in Kapitel 8 beschrieben Konfigurationen des EVG.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten krypthographischen Algorithmen (vgl. §9 Abs. 4 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

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:

CARD STAR /memo3, FW-Version 4.0.6, HW-Versionen B00/B01

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	HW	Terminal CARD STAR /memo3	B01[7]	In Umverpackung
2	SW	Firmware 4.0.6	4.0.6	Installiert bei Auslieferung
3	SW	Updatedatei Memo3_4-0-6_FGOG00026.upd Hashwert (SHA-256): 7192DFFF3AB578ECAD7D30048527CED6ECBDE73AC43AFDC00ECB351EA1B5E4DF	4.0.6	Auf Anfrage beim Hersteller; nur im Rahmen der Erprobungsphase ORS1
4	SW	Updatedatei Memo3_4-0-6_FGOG00026(InitialORS1).upd Hashwert (SHA-256): 58413C303ABC0717548BDA9863E39D9699A7726250120DEA12C5ABFE132CECFA	4.0.6	Auf Anfrage beim Hersteller; nur im Rahmen der Erprobungsphase ORS1
5	DOC	Bedienungsanleitung [10] Hashwert (SHA-256): B57E660C719BF5A8C704F28F33FB21F7F1B7C7118C3362EF8B66BC2E2DB34811	27.07.2017	Auf Anfrage beim Hersteller; nur im Rahmen der Erprobungsphase ORS1

Tabelle 2: Auslieferungsumfang des EVG

Der EVG wird im vorstehend angegebenen Umfang in einer Umverpackung ausgeliefert, die alle genannten Bestandteile enthält.

Die Auslieferung erfolgt durch zwei Mitarbeiter der CCV Deutschland GmbH (Firmenkuriere) an die Lieferadresse und die benannte Person des Leistungserbringers (Direktlieferung). Die Mitarbeiter von CCV überprüfen den Personalausweis des Empfängers um dessen Identität zu verifizieren. Die Mitarbeiter von CCV lassen sich die korrekte Auslieferung vom Empfänger schriftlich bestätigen.

[7] Der EVG wird nicht mehr in der Hardwareversion B00 ausgeliefert.

Während der Versandabwicklung wird für jede Bestellung eine individuelle Lieferankündigung erzeugt und per Post versendet. Die Lieferankündigung enthält folgende Informationen:

- Avisierter Liefertermin, wann die Lieferung erfolgt (Datum und ungefähre Uhrzeit);
- Namen der CCV Mitarbeiter, die die Auslieferung vornehmen;
- Seriennummer des Gerätes / der Geräte;
- Link auf die im Internet hinterlegten signierten Anleitungen mit Hinweis, dass die Sicherheitshinweise vorab zu lesen sind;
- Informationen, wie und was beim Empfang des Terminal zu überprüfen ist.

Der Empfänger überprüft die Korrektheit der Lieferung und des EVG

- durch Überprüfen der Personalien des Firmenkuriers;
- durch Prüfung der fälschungsgeschützten Siegel mit BSI-Zertifizierungskennung und weiteren Sicherheitsmerkmalen; das Gerät soll nicht verwendet werden, wenn ein Siegel bei Empfang nicht intakt ist, und der Hersteller ist zu kontaktieren;
- durch Prüfung der Seriennummer des Gerätes (Seriennummernaufkleber und Prüfung laut Bedienungsanleitung). Sollte die Seriennummer des gelieferten Gerätes von der Lieferankündigung abweichen, darf das Gerät nicht verwendet werden, und der Hersteller ist zu kontaktieren.

Die vom Empfänger zu prüfenden Angaben wurden dem Empfänger zuvor als Lieferankündigung per Post übersandt.

Die zertifizierte Firmware in der Version 4.0.6 hat den Hashwert (SHA-256) 7192DFFF3AB578ECAD7D30048527CED6ECBDE73AC43AFDC00ECB351EA1B5E4DF.

Für das Update von einer Firmwareversion Q1.03 auf die Firmware des EVGs (4.0.6) wird die Update-Datei mit dem Dateinamen Memo3_4-0-6_FGOG00026(InitialORS1).upd und dem Haswert (SHA-256) 58413C303ABC0717548BDA9863E39D9699A7726250120DEA12C5ABFE132CECFA benötigt.

Die Firmwareversion kann über eine Info-Funktion auf der Anzeige des EVG angezeigt werden.

3. Sicherheitspolitik

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

Die Versichertendaten werden im EVG nur vorübergehend und nur verschlüsselt gespeichert. Zur Anzeige und zum Auslesen von Versichertendaten wird ein Berechtigungskonzept durchgesetzt. Administrative Funktionen werden von allen weiteren Funktionen unterschieden. Administrative Funktionen, die Sicherheitsaspekte berühren, können nur nach vorheriger Authentisierung ausgeführt werden.

Details zu einzelnen Aspekten der Sicherheitspolitik können dem Abschnitt 3 der Sicherheitsvorgaben [6] entnommen werden.

4. Annahmen und Klärung des Einsatzbereiches

Die in den Sicherheitsvorgaben definierten Annahmen sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte führen zu Sicherheitszielen, die durch die EVG-Einsatzumgebung erfüllt werden müssen. Hierbei sind die folgenden Punkte relevant:

- OE.MEDIC: The medical supplier shall be non hostile, always act with care, and read the existing guidance documentation of the TOE.
- OE.ADMIN: The administrator shall be non hostile, always act with care, read the existing guidance documentation of the TOE and adhere to the rules of the TOEs environment.
- OE.Developer: The developer is assumed to be non hostile, always act with care and knows the existing guidance documentation of the TOE.
- OE.CARDS: The authorised cards and the eHC are smart cards that comply with the specification of the gematik.
- OE.DMS: The TOE shall only be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier.
- OE.PHYSICAL: The secure TOE environment shall protect the TOE against physical manipulation.
- OE.ENVIRONMENT: While the TOE is in use by either the medical supplier or the administrator, they always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE is not in use, it is kept in a secure area.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5. Informationen zur Architektur

Das CARD STAR /memo3 ist ein mobiles, handliches Gerät, das der Erfassung, Speicherung und Übertragung an ein PVS von Versichertendaten dient. Die Firmware des Gerätes, Version 4.0.6, ist ein monolithisches Image, das alle erforderlichen Funktionen bereitstellt. Ein besonderes Betriebssystem wird nicht benötigt, da die Firmware auch alle Hardwarekomponenten ansteuert.

Die Firmware ist modular aufgebaut, wobei folgende Subsysteme unterschieden werden können:

- Die generelle Ablaufsteuerung erfolgt im Subsystem s_ctrl, das auch die grundlegenden Funktionen zur Ansteuerung der Hardware bereitstellt.
- Das Subsystem s_lib stellt häufig benötigte Bibliotheksfunktionen zur Verfügung.
- Die Kommunikation mit den Kartentypen eGK, KVK, SMC-B und HBA wird vom Subsystem s_card realisiert.
- Die Übertragung gespeicherter Daten an ein PVS und die Updatefunktionalität werden vom Subsystem s_comm bereitgestellt.
- Die Abwicklung der Benutzerinteraktionen, bei der Anzeigen auf dem Display erfolgen und Eingaben auf der Tastatur vorzunehmen sind, obliegt dem Subsystem s_user.

Bei einem Firmwareupdate werden nicht einzelne Subsysteme aktualisiert, sondern stets die gesamte Firmware.

6. Dokumentation

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

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

7. Testverfahren

Die Anforderungen an die Einsatzumgebung werden im Abschnitt 1.2.2 von [8] wie folgt definiert (Zitat):

- This Protection Profile specifies the security needs for the MobCT in a secure operational environment where protection against physical manipulation of the TOE is covered by the TOE environment.
- The TOE will be locked in a secure area whenever it is not used. The secure area is only accessible for the medical supplier and persons authorised by them. Intrusion to the secure area for the TOE will be easily detectable by the medical supplier. In such a case the device will not be used anymore and will have to be replaced.
- The medical supplier is considered to know the user guidance for his TOE and operate it accordingly.

7.1. Herstellertests

Der EVG wurde in der in den Sicherheitsvorgaben [6] angegebenen Konfiguration mit der Firmwareversion 4.0.6 und der Hardwareversion B01 getestet. Die Testergebnisse sind auf die Hardwareversion B00 übertragbar.

Um die vom EVG bereitgestellten Sicherheitsfunktionen zu testen, hat der Entwickler eine Vielzahl von Tests spezifiziert und durchgeführt. Von den in den Sicherheitsvorgaben [6] definierten sieben Sicherheitsfunktionen sind sechs implementiert; die sichere Anzeige von Notfalldaten ist derzeit nicht implementiert, da die Notfalldaten noch nicht spezifiziert sind.

Jede der sechs implementierten Sicherheitsfunktionen wurde mit mindestens fünf Tests geprüft. Die Ergebnisse der durchgeführten Tests entsprachen in jedem Fall dem erwarteten Verhalten des EVGs. Hinweise auf eine eventuell fehlerhafte Implementierung von Sicherheitsfunktionen wurden dabei nicht gefunden. Darüber hinaus hat der Hersteller umfangreiche Tests im Rahmen der Zulassung des EVG durch die gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH durchgeführt.

Insgesamt zeigen die Tests, dass sich der EVG wie in den Sicherheitsvorgaben [6], in der Funktionalen Spezifikation und dem Entwurf auf hoher Ebene spezifiziert verhält.

7.2. Unabhängige Prüfstellentests

Die unabhängige Tests der Prüfstelle wurden mit mehreren Versionen der Firmware (Versionen 4.0.1, 4.0.5 und 4.0.6) und der Hardware B01 durchgeführt. Insgesamt zeigen die Tests, dass sich der EVG verhält, wie in den Sicherheitsvorgaben [6], in der Funktionalen Spezifikation und dem Entwurf auf hoher Ebene spezifiziert.

Bei den unabhängigen Tests wurden insbesondere die Updatefunktionalität und die Schnittstelle zur elektronischen Gesundheitskarte getestet. Jede Sicherheitsfunktion wurde mit mindestens einem speziellen Test geprüft.

7.3. Schwachstellenanalyse

Die Schwachstellenanalyse wurde in Übereinstimmung mit den Anforderungen der Vertrauenswürdigkeitskomponente AVA_VAN.5 als fortgeschrittene, methodische Schwachstellenanalyse durchgeführt (advanced methodical vulnerability analysis). Sie umfasste die Suche nach potentiellen Schwachstellen in einschlägigen öffentlich verfügbaren Quellen, die unabhängige, systematische Analyse aller für den EVG gelieferten Informationen und Dokumente und die Durchführung von Penetrationstests zur Bestätigung oder Widerlegung von Hypothesen über potentielle Schwachstellen.

Indem die Schwachstellenanalyse durchgeführt wurde, stellten die Evaluatoren fest, dass der EVG keine ausnutzbaren Schwachstellen aufweist.

Restliche Schwachstellen („residual vulnerabilities“) können aus der theoretischen Analyse und Penetrationstests, die bezüglich der identifizierten Angriffsszenarien definiert wurden, resultieren. Indem die Schwachstellenanalyse durchgeführt wurde, stellten die Evaluatoren fest, dass der EVG keine restlichen Schwachstellen aufweist.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG: Der EVG liegt in zwei Hardware-Bauarten vor, B00 und B01, die sich bezüglich der Dimensionierung einiger passiver Bauelemente unterscheiden.

Die Firmware wurde in der Version 4.0.6 evaluiert.

Die Einsatzumgebung unterliegt, soweit der EVG nicht im Betrieb ist, folgender Beschränkung: „The TOE will be locked in a secure area whenever it is not used. The secure area is only accessible for the medical supplier and persons authorised by them. Intrusion to the secure area for the TOE will be easily detectable by the medical supplier. In such a case the device will not be used any more and will have to be replaced.”

Ein unbeaufsichtigter Betrieb des EVG ist nicht zulässig. Die Nutzung der Dockingbetriebsart gehört NICHT zum geprüften Funktionsumfang.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 1.4.

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

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

Die Evaluierungsmethodologie CEM [2] wurde verwendet.

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

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die zusätzlichen Komponenten
  ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 und AVA_VAN.5

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 19 January 2015 [8]
- Funktionalität: PP konform
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 3 mit Zusatz von ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 und AVA_VAN.5

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

Die kryptografische Algorithmenstärke wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 100 Bit nicht länger als sicher angesehen werden, ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden, ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der 'Technischen Richtline BSI TR-02102' (https://www.bsi.bund.de) entnommen werden.

Die folgende Tabelle gibt einen Überblick über die zur Durchsetzung der Sicherheitspolitik im EVG enthaltenen kryptographischen Funktionalitäten und legt deren Bewertung des Sicherheitsniveaus aus kryptographischer Sicht dar. Jede kryptografische Funktion, die in der Spalte 'Sicherheitsniveau mehr als 100 Bit' ein 'Nein' enthält erreicht nur ein Sicherheitsniveau unterhalb von 100 Bit (im allgemeinen Anwendungsfall).

Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüssel-größe in Bits	Sicherheits-niveau mehr als 100 Bit
Authentizität und Integrität	Verifikation von RSASSA-PKCS1-v1_5 Signaturen mit SHA-256 Hashfunktion	PKCS#1 (RSA), FIPS 180-4 (SHA)	2048	Ja

Tabelle 3: Kryptografische Funktionen des EVG

Die folgende Tabelle gibt einen Überblick über die zur Durchsetzung der Sicherheitspolitik im EVG enthaltenen kryptographischen Funktionalitäten und verweist auf den jeweiligen Anwendungsstandard in dem die Eignung festgestellt ist.

Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüssel-größe in Bits	Anwendungsstandard
Vertraulichkeit und Integrität	AES im GCM-Modus	FIPS-197 (AES), NIST SP 800-38D (AES-GCM)	256	gemSpec_Krypt [11]

Tabelle 4: Kryptografische Funktionen des EVG

Die kryptografische Stärke dieser Algorithmen wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2).

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.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen wie in Kapitel 9 dargelegt muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

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.

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

- Das stationäre Kartenlesegerät CARD STAR /medic2 des Herstellers kann als Dockingstation für den EVG dienen, mit dessen Hilfe erfasste Versichertendaten ebenfalls an ein PVS übertragen werden können. Diese Betriebsart ist NICHT evaluiert worden. Die Nutzung der Dockingstation zum Übertragen von Daten an ein PVS erfolgt auf eigene Verantwortung des Benutzers.

11. Sicherheitsvorgaben

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

12. Definitionen

12.1. Abkürzungen

AES Advanced Encryption Standard

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

C2C Card-toCard-Authentifizierung

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

CT Card Terminal

DMS Data Management System (Primärsystem)

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

eGK Elektronische Gesundheitskarte

eHC Electronic Health Card

eHCT Electronic Health Card Terminal

ETR Evaluation Technical Report

EVG Evaluierungsgegenstand

gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

HBA Heilberufsausweis

HPC Health Professional Card (identisch HBA)

IT Information Technology - Informationstechnologie

ITSEF Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit

KVK KrankenVersichertenKarte

MobCT Mobile Health Card Terminal

PP Protection Profile - Schutzprofil

PVS Praxisverwaltungssystem

RTC Real Time Clock (Echtzeituhr)

SAR Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen

SF Security Function - Sicherheitsfunktion

SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
SMC	Secure Module Card (Institutskarte)
ST	Security Target - Sicherheitsvorgaben
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality - EVG-Sicherheitsfunktionalität

12.2. Glossar

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

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

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

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

Informell - Ausgedrückt in natürlicher Sprache.

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

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

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

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

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

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

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

13. Literaturangaben

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1
Part 1: Introduction and general model, Revision 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[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] Sicherheitsvorgaben BSI-DSZ-0689-V2-2018, Version 3.00, 25.01.2018, CARD STAR /memo3 - Security Target, CCV Deutschland GmbH

[7] Evaluierungsbericht, Version 1.3, 01.06.2018, Evaluation Technical Report - Zusammenfassung (Summary): BSI-DSZ-CC-0689V2, datenschutz cert GmbH (vertrauliches Dokument)

[8] Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), BSI-CC-PP-0052, Version 1.4, 24.09.2014, Bundesamt für Sicherheit in der Informationstechnik

[9] Konfigurationsliste für den EVG, Version 1.00, 16.04.2018, CARD STAR Terminals - Konfigurationselemente (vertrauliches Dokument)

[10] Dokumentation für den EVG, Version vom 27.07.2017, Mobiles Kartenterminal für eGK und KVK, Bedienungsanleitung

[11] Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gemSpec_Krypt, Version 2.3.0, 17.06.2014, gematik

Referenzierte Standards:

[FIPS 180-4] FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST, 2012-03

[FIPS 197] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard, October 2012

[NIST SP 800-38D] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)

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 10.4
- 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 11
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC Teil 3 Kapitel 12 bis 16
- 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 http://www.commoncriteriaportal.org/cc/ veröffentlicht.

Dies ist eine eingefügte Leerseite.

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Bemerkung: Ende des Reportes