Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1159-2021

zu

ePA Modul Frontend des Versicherten, v1.0.7

der

CompuGroup Medical Deutschland AG

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-1159-2021 (*)

ePA Modul Frontend des Versicherten
v1.0.7

von	CompuGroup Medical Deutschland AG
PP-Konformität:	None
Funktionalität:	Produktspezifische Sicherheitsvorgaben Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 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.

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

Common Criteria
Recognition Arrangement

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

Bonn, 27. August 2021
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola 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

A. Zertifizierung

1. Vorbemerkung

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

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

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

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

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

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

2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), 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 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 ePA Modul Frontend des Versicherten, v1.0.7 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts ePA Modul Frontend des Versicherten, v1.0.7 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 20. August 2021 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Antragsteller ist: CGM.

Das Produkt wurde entwickelt von: CGM.

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

5. Gültigkeit des Zertifizierungsergebnisses

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

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

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

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

[5] Information Technology Security Evaluation Facility

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 27. August 2021, ist gültig bis 26. August 2026. 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 ePA Modul Frontend des Versicherten, v1.0.7 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] CGM
Maria Trost 21
56070 Koblenz
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 EVG hat die Bezeichnung ePA Modul FdV (Frontend des Versicherten) und wurde in Version v1.0.7 evaluiert. Der EVG ist ein ePA (elektronische Patientenakte) Modul für ein FdV (Frontend des Versicherten), das entsprechend [10] implementiert ist. Der EVG ist als Softwarepaket implementiert, das in eine Anwendung integriert werden kann, welche dann auf einem Android oder iOS Endgerät ausgeführt wird.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie verwenden kein zertifiziertes Protection Profile.

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 2.

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

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

Sicherheitsfunktionalität des EVG	**Thema**
IdentifierSF.SelfProtection	Selbstschutz des EVG
SF.CryptographicServices	Kryptographische Dienste
SF.TSL	Trust Service Status List
SF.TLS	TLS Service
SF.VAU-Server-Protokoll	VAU Server Protokoll
SF.SGD	SGD Protokoll / ECIES
SF.EGK	eGK Kommunikation
SF.SIGD	SIGD Kommunikation

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 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

Es gibt nur eine Konfiguration des EVG. Für mehr Details siehe Kapitel 8.

Die Ergebnisse der Schwachstellenanalyse, wie in diesem Zertifikat bestätigt, erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten kryptographischen 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:

ePA Modul Frontend des Versicherten, v1.0.7

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	SW	ePA Modul FdV	Version: v1.0.7, git Commit ID: b8e91a8be0 21ec111689 f9f2cebd12 d0aaa61b2e	Geteiltes git Repository, auf das der Integrator BRICKMAKERS zugreifen kann
2	DOC	Guidance Documents ePA Modul Frontend des Versicherten	1.10	Nextcloud Server von os-cillation
3	DOC	epa-fdv-flutter-plugin_v1.0.7-doxygen	SHA-256 Hashwert: 0525059930A722048C13D91 D641B47723B1315BFFFC377 75D60BA612DAFADC6D	
4	DOC	epa-fdv-modul_v1.0.7-doxygen	SHA-256 Hashwert: CCCA0D64DD5F5529EED78 FF6194750B4C501B7B83BE1 B52D1B17CD01DEFC7C49	
5	DOC	Funktionale Spezifikation ePA Modul Frontend des Versicherten	1.19	

Tabelle 2: Auslieferungsumfang des EVG

Die Auslieferung des EVG als Softwarekomponente an BRICKMAKERS wird durch ein zwischen os-cillation und BRICKMAKERS geteiltes git Repository realisiert. In diesem Repository werden die im TOE enthaltenen C++-Bibliotheken in kompilierter Form zusammen mit einem Plugin für Flutter/Dart abgelegt. Die Auslieferung der Dokumentation an den Benutzer wird durch einen Nextcloud Server von os-cillation realisiert. Der Benutzer verifiziert die Version der funktionalen Spezifikation und des Handbuchs durch Vergleich mit den Angaben in diesem Zertifizierungsbericht. Die Integrität der Doxygen-Dokumentation kann durch Hashwerte geprüft werden. Der EVG muss nicht installiert werden, da es sich um C++ Bibliotheken handelt, die über das bereitgestellte Plugin in eine Anwendung integriert werden. Der EVG wird mithilfe automatisierter Build-Tools in eine Anwendung integriert. Dies ist eine Standardprozedur zur Integration von

Softwarebibliotheken in Anwendungen für die zugrundeliegenden Plattformen (iOS und Android). Die Bibliotheken müssen so verwendet werden, wie im Handbuch beschrieben.

3. Sicherheitspolitik

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

- Kryptographische Unterstützung,
- Schutz von Benutzerdaten,
- Schutz der TSF und
- Vertrauenswürdiger Pfad/Kanal.

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.Secure.TI: Sichere Telematikinfrastruktur-Plattform,
- OE.Secure.eGK: Sichere eGK,
- OE.Secure.KVS: Sicheres KVS,
- OE.Secure.SigD: Sicherer SigD,
- OE.KeyStorage: Vertrauenswürdiger Schlüsselspeicher,
- OE.Correct.GUI: Korrekte TOE-Nutzung durch FdV,
- OE.NonMalicious.Dev: Nicht böswilliger FdV-Entwickler,
- OE.Secure.Device: Sichere Verwaltung GdV und
- OE.Integr.FdV: Schutz des Vertrauensankers der Telematikinfrastruktur.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.

5. Informationen zur Architektur

Der EVG umfasst die folgenden beiden Subsysteme, die wiederum aus mehreren Modulen bestehen:

- Subsystem C++ Core:
  Es stellt die Fachlogik-Aufrufe sowie die kryptographischen Verfahren bereit, mit denen Anwendungsfälle zum Aktensystem in der TI-Infrastruktur bearbeitet werden können. Es verwaltet Aufrufe an den externen Signaturdienst und an das Kontoverwaltungssystem zur Verwendung einer alternativen Versichertenidentität. Funktionen zur PIN-Eingabe und Entropieerzeugung werden durch das Subsystem realisiert.
- Subsystem Flutter-Plugin:
  Es stellt die Schnittstelle LS.FdV zur Verfügung und gewährleistet damit die Anbindung des ePA Modul FdV an die umgebende Anwendung ePA Frontend des

Versicherten. Um die Verwendung sowohl unter Android als auch in iOS zu gewährleisten, wird das Plugin im Framework ”Flutter” umgesetzt.

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. Herstellertests

Die Tests wurden mit dem EVG ePA Modul FdV in der einzigen Konfiguration des EVGs durchgeführt.

Der Hersteller hat die folgenden Aspekte bei der Erstellung des Testkonzepts berücksichtigt:

- Tests um alle Aktionen und Schnittstellen die in der funktionalen Spezifikation definiert sind abzudecken, außer TSFIs LS.AUTHORIZATION und LS.SECURE_STORAGE. Diese TSFIs werden indirekt durch andere Tests abgedeckt. TSFI LS.SECURE_STORAGE ist in jedem Test bezüglich Kommunikation per TLS, VAU Protokoll oder SGD Protokoll involviert, da alle Sitzungsdaten in dem sicheren Speicher abgelegt werden. Durch TSFI LS.AUTHORIZATION werden der Autorisierungsschlüssel und -token für den EVG bereitgestellt. Diese Daten werden benötigt um einen Kommunikationskanal mit der Dokumentenverwaltungskomponente aufzubauen. Daher wird LS.AUTHORIZATION implizit durch die Tests auf TSFI LS.DOCUMENT_MANAGEMENT getestet.
- Unit Tests für Gut- und Schlechtfälle der EVG-Sicherheitsfunktionalität.
- Tests der kryptographischen Funktionalität durch Testvektoren und Gutfall- sowie Schlechtfall-Tests der implementierten Protokolle.
- Testfälle, die durch die gematik implementiert sind und ein simuliertes ePA-Aktensystem verwenden.

Ergebnis:

Alle Testfälle wurden erfolgreich für die finale Version des EVG ausgeführt.

Die Ergebnisse der Herstellertests zeigen, dass der EVG so funktioniert wie erwartet.

7.2. Unabhängige Prüfstellentests

Testansatz und Testaufbau:

Der EVG ist das ePA Modul FdV. Der Evaluator hat alle TSF mithilfe einer Reihe von Testfällen getestet, wobei jeder Testfall einen speziellen Aspekt des erwarteten EVG-Verhaltens abdeckt. Die TSF werden durch Unit Tests getestet oder indem Testskripte in der Testumgebung an der EVG-Schnittstelle ausgeführt wurden. Die TSF werden in den

Testskripten stimuliert, das Verhalten des EVG als Rückgabewert aufgezeichnet und mit dem erwarteten Wert innerhalb der Testskripte verglichen.

Die Tests werden durch eine Testsoftware mithilfe von Testskripten durchgeführt. Testattribute, Vorbedingungen und Nachbearbeitungen sind in den Testskripten enthalten, um zu gewährleisten, dass die Ausführung der Skripte reproduzierbar ist. Die Testumgebung wird durch den Hersteller gestellt und die Testskripte wurden durch den Hersteller implementiert nach Testspezifikation des Evaluators.

In der Sicherheitsvorgabe [6] ist nur eine Konfiguration des EVG definiert. Die Unit Tests sind im Quellcode enthalten und in den Build-Prozess integriert und testen daher direkt die einzig mögliche Konfiguration. Für die Testfälle, die auf die externen Schnittstellen des EVG abzielen, wurde ein Testtreiber in C++ implementiert, um den EVG als Bibliothek laden zu können und die externen Schnittstellen für Testskripte verfügbar zu machen.

Die Personalisierungsdaten, die in der Testkonfiguration verwendet wurden, wurden durch den Hersteller bereitgestellt.

Alle Herstellertests und alle Prüfstellentests wurden mit der finalen Version des EVG durchgeführt.

Testergebnisse:

Die Testergebnisse haben keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen aufgezeigt.

7.3. Penetrationstests der Prüfstelle

Die Penetrationstests wurden in der Testumgebung des Herstellers unter Aufsicht des Evaluators durchgeführt. Der EVG wurde unter Aufsicht des Evaluators entsprechend des Handbuchs konfiguriert. Das zusammenfassende Ergebnis ist, dass es keine Abweichungen zwischen den erwarteten und tatsächlichen Testergebnissen gab. Kein Angriffsszenario mit Angriffspotenzial Basic war erfolgreich.

Penetrationstestansatz:

Der Evaluator entwickelte die Angriffsszenarien für die Penetrationstests auf Basis einer Liste von potenziellen Schwachstellen, welche auf den EVG in seiner operativen Einsatzumgebung zutreffen, unter der Annahme, dass diese potenziellen Schwachstellen in der operativen Einsatzumgebung ausnutzbar sein könnten. Dabei hat er auch alle Aspekte der Sicherheitsarchitektur des EVG berücksichtigt, die nicht durch funktionale Herstellertests abgedeckt sind.

Der Fokus beim Entwickeln der Penetrationstests lag darauf, alle potenziellen Schwachstellen, die auf den EVG in seiner operativen Einsatzumgebung zutreffen, abzudecken.

Ergebnis:

Das zusammenfassende Ergebnis ist, dass es keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen gab. Kein Angriffsszenario mit Angriffspotenzial Basic war erfolgreich in der operativen Einsatzumgebung wie sie in den Sicherheitsvorgaben beschrieben ist unter der Annahme, dass alle dort geforderten Maßnahmen umgesetzt sind.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die in Abschnitt 1 und im ST [6], Abschnitt 1.3 beschriebene Konfiguration des EVG.

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.

Für die Analyse des Zufallszahlengenerators wurde AIS 20 verwendet, siehe [4].

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

- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 2 der CC (siehe auch Teil C des Zertifizierungsreports)

Die Evaluierung hat gezeigt:

- PP Konformität: None
- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform EAL 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

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 verweist auf den jeweiligen Anwendungsstandard in dem die Eignung festgestellt ist.

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungs-standard	Kommentar
Vertrauenswürdiger Kanal	TLS v1.2 Erlaubte Cipher Suites: TLS_ECDHE_RSA_WITH_AES_128_GCM_	[RFC5246]	128, 256 (AES) 2048 (RSA) EC Schlüssellängen gemäß der	[TR-03116-1]	FCS.CKM.1/TLS, FCS_COP.1/TLS.AES, FCS_COP.1/TLS.Auth.RSA, FCS_COP.1/TLS.A

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungs-standard	Kommentar
	SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECSDA_WITH_AES_128_GCM_SHA256		verwendeten elliptischen Kurven brainpoolP256r1, P-256		uth.ECDSA, FCS_COP.1/TLS.Hash, FCS_COP.1/TLS.HMAC, FPT_TDC.1/TLS.Zert, FTP_ITC.1/TLS
Vertrauenswürdiger Kanal	TLS v1.3 Erlaubte Cipher Suites: TLS_AES_128_GCM_SHA256	[RFC8446]	128 (AES)	[TR-03116-1]	FCS.CKM.1/TLS, FCS_COP.1/TLS.AES, FCS_COP.1/TLS.Auth.RSA, FCS_COP.1/TLS.Auth.ECDSA, FCS_COP.1/TLS.Hash, FCS_COP.1/TLS.HMAC, FPT_TDC.1/TLS.Zert, FTP_ITC.1/TLS
Vertrauenswürdiger Kanal	ECIES Erlaubte Cipher Suites: ECDH_ECDSA_WITH_AES_256_GCM_SHA256	[gemSpec_Krypt]	256 (AES) EC Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1	-	FTP_ITC.1/SGD, FCS_COP.1/SGD.ECIES, FCS_COP.1/SGD.ECDSA, FCS_COP.1/SGD.Hash, FCS_COP.1/AES, FPT_TDC.1/SGD.Zert
Vertrauenswürdiger Kanal	JWS Erlaubte Cipher Suites: ECDSA_SHA256	[RFC7515]	Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1, P-256	-	FCS_CKM.1/JWS.Keys, FCS_CKM.2/JWS.ECDSA, FCS_COP.1/JWS.ECDSA, FTP_ITC.1/JWS
Vertrauenswürdiger Kanal	VAU-Protokoll Erlaubte Cipher Suites: ECDH_ECDSA_WITH_AES_256_GCM_SHA256	[gemSpec_Krypt]	256 (AES) EC Schlüssellängen gemäß der verwendeten elliptischen Kurve brainpoolP256r1	-	FCS_CKM.1/VAU, FCS_COP.1/VAU.AES, FCS_COP.1/VAU.ECDSA, FCS_COP.1/VAU.HASH, FPT_TDC.1/VAU.Zert, FTP_ITC.1/VAU

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungs-standard	Kommentar
Vertrauenswürdiger Kanal	PACE - Secure Messaging Erlaubte Cipher Suites: AES_CBC_{128,192,256}, SHA-1, SHA-{256,384,512}, ECDH, AES_CMAC_{128,192,256} ID_PACE_ECDH_GM_AES_CBC_CMAC_128 ID_PACE_ECDH_GM_AES_CBC_CMAC_192 ID_PACE_ECDH_GM_AES_CBC_CMAC_256	[ISO_7816]	128, 192, 256 (AES) EC Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	[TR-03110-2]	FCS_COP.1/SM.SHA, FCS_COP.1/SM.AES, FCS_CKM.1/SM, FCS_CKM.1/PACE, FCS_COP.1/SM.CMAC, FTP_ITC.1/SM
Vertraulichkeit/ Integrität/ Authentizität	AES im GCM Modus	[FIPS197] (AES) [NIST SP800-38D] (GCM)	128, 256	[TR-03116-1]	FCS_COP.1/AES
Vertraulichkeit	AES im CBC Modus	[FIPS197] (AES)	128, 192, 256	[TR-03116-1]	FCS_COP.1/SM.AES
Integrität/ Authentizität	CMAC	[NIST SP800-38B]	128, 192, 256	[TR-03116-1]	FCS_COP.1/SM.CMAC
Authentizität/ Authentisierung	RSASSA- PKCS1-v1_5 / RSASSA-PSS	[RFC8017] (RSA) [FIPS180-4] (SHA)	Modulus Länge= 2048	[TR-03116-1]	FCS_COP.1/TLS.Auth.RSA
Authentizität	ECDSA-Signaturerzeugung mit SHA-256/384	[FIPS186-2] (ECDSA) [RFC5639] / [RFC7027] (brainpool) [FIPS186-4] (NIST Kurven) [FIPS180-4] (SHA)	Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1, brainpoolP384r1, P-256, P-384	[TR-03116-1]	FCS_COP.1/TLS.Auth.ECDSA, FCS_COP.1/VAU.ECDSA, FCS_COP.1/SGD.ECDSA, FCS_COP.1/JWS.ECDSA

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungs-standard	Kommentar
Authenti-sierung	ECDSA-Signaturverifikation mit SHA-256	[FIPS186-4] (ECDSA) [RFC5639] / RFC 7027(brainpool) [FIPS186-4] (NIST Kurven) [FIPS180-4] (SHA)	Schlüssellängen gemäß der verwendeten elliptischen Kurve brainpoolP256r1	[TR-03116-1]	FCS_COP.1/ TLS.Auth.ECDSA, FCS_COP.1/VAU. ECDSA, FCS_COP.1/SGD. ECDSA, FCS_COP.1/JWS. ECDSA
Schlüsselaustausch	ECDH für TLS, VAU Protokoll und ECIES	[TR-03111] / NIST SP 800-56-A (ECDH) [RFC5639] / RFC 7027(brainpool) [FIPS186-4] (NIST Kurven)	Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1, brainpoolP384r1, P-256, P-384	[TR-03116-1]	FCS_CKM.1/VAU, FCS_CKM.1/TLS, FCS_COP.1/SGD. ECIES
Schlüsselaustausch	ECDH für PACE	[TR-03111] / [NIST SP800-56A] (ECDH) [RFC5639] / [RFC7027] (brainpool) [FIPS-186-4] (NIST Kurven)	Schlüssellängen gemäß der verwendeten elliptischen Kurven brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	[TR-03110-2]	FCS_CKM.1/ PACE
Zufalls-zahlener-zeugung	Deterministischer Zufallszahlengenerator gemäß DRG.3	[AIS20], [NIST SP800-90A]	-	[TR-03116-1]	FCS_CKM.1/Dok-Schlüssel, FCS_CKM.1/JWS. KEYS, FCS_CKM.1/PAC E, FCS_CKM.1/TLS, FCS_CKM.1/VAU, FCS_RNG.1
Integrität/ Authentizität	HMAC mit SHA-256, SHA-384	[RFC2404] (HMAC) [FIPS180-4] (SHA)	256, 384	[TR-03116-1]	FCS_COP.1/ TLS.HMAC
Integrität (OCSP)	SHA-1	[FIPS180-4] (SHA) [RFC6960] (OCSP)	160	[TR-03116-1]	FCS_COP.1/ VAU.HASH, FCS_COP.1/TLS. Hash

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungs-standard	Kommentar
Integrität	SHA-256, SHA-384	[FIPS180-4] (SHA)	256, 384	[TR-03116-1]	FCS_COP.1/ OAUTH.HASH, FCS_COP.1/TLS. Hash, FCS_COP.1/SGD. Hash
Integrität	SHA-1, SHA-256, SHA-384, SHA-512	[FIPS180-4] (SHA)	128, 256, 384, 512	[TR-03116-2]	FCS_COP.1/ SM.SHA, FCS_COP.1/VAU. HASH, FCS_COP.1/TLS. Hash, FCS_COP.1/OAUT H.HASH, FCS_COP.1/SGD. Hash
Schlüsselableitung	HKDF (HMAC-SHA256)	[RFC5869] (HKDF) [FIPS180-4] (SHA)	256	[gemSpec_Krypt]	FCS_COP.1/ TLS.HMAC, FCS_COP.1/TLS. Hash

Tabelle 3: kryptografische Funktionen des EVG

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

Gemäß [gemSpec_Krypt], [TR-03110-2] und [TR-03116-1] sind die Algorithmen für den jeweiligen Zweck geeignet.

Eine explizite Gültigkeitsdauer wird nicht angegeben.

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.

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
al.vi	alternative Versichertenidentität
API	Application Programming Interface
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
DRNG	Deterministic RNG
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
eGK	Elektronische Gesundheitskarte
ePA	elektronische Patientenakte
EVG	Evaluierungsgegenstand
ETR	Evaluation Technical Report
FdV	Frontend des Versicherten
GdV	Gerät des Versicherten
GUI	Grafische Benutzeroberfläche
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
JWS	JSON Web Signatures
KVS	Kontoverwaltungssystem
OCSP	Online Certificate Status Protocol

OSP	Organizational Security Policy
PACE	Password Authenticated Connection Establishment
PP	Protection Profile – Schutzprofil
RNG	Random Number Generator
SAR	Security Assurance Requirement - Vertrauenswürdigkeitsanforderungen
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
SGD	Schlüsselgenerierungsdienst
SHA	Secure Hash Algorithm
ST	Security Target – Sicherheitsvorgaben
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
TSL	Trust-service Status List
VAU	vertrauenswürdige Ausführungsumgebung
VZD	Verzeichnisdienst

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[7] 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-CC-1159-2021, Version 1.29, 18.07.2021, Security Target ePA Modul Frontend des Versicherten Version v1.0.7, CGM AG

[7] Evaluierungsbericht, Version 2, 18.08.2021, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH (vertrauliches Dokument)

[7] specifically

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[8] Konfigurationsliste für den EVG, Version 1.0.7, epa-fdv-modul_v1.0.7-items.csv (vertrauliches Dokument)

[9] Dokumentation für den EVG, Version 1.10, 18.07.2021, Guidance Documents ePA Modul Frontend des Versicherten

[10] Referenzen auf Anwendungsstandards: [gemProdTePAModulFdV] Produkttypsteckbrief des ePA Frontends des Versicherten. Prüfvorschrift. Produkttyp Version PTV1 1.1.0-0. Version 1.0.0., 5. November 2020

[gemSpec_Krypt] Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik, Version 2.16.2, 05. November 2020.

[TR-03110-2] BSI - Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.21, 2016-12-21, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03111] BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.0, 2012-06-28, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03116-1] Technische Richtlinie BSI TR-03107-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20, 2018-09-21, Bundesamt für Sicherheit in der Informationstechnik.

[11] Referenzen von Implementierungsstandards:

[FIPS180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[FIPS197] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST).

[ISO_7816-4] ISO/IEC 7816-4:2013 – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, International Organization for Standardization.

[NIST SP800-38B] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST).

[NIST SP800-38D] NIST SP800-38D, Recommendation for Block Cipher Modes of

Operation: Galois/Counter Mode (GCM) and GMAC, 2007-11, National Institute of Standards and Technology (NIST).

[NIST SP800-56A] NIST SP800-56A, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Revision 3, 2018-04, National Institute of Standards and Technology (NIST).

[NIST SP800-90A] NIST SP800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, 2015-06, National Institute of Standards and Technology (NIST).

[RFC2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997 (https://www.ietf.org/rfc/rfc2104.txt).

[RFC2404] RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH, November 1998 (https://www.ietf.org/rfc/rfc2404.txt)

[RFC5246] RFC 5246 - The Transport Layer Security (TLS) Protocol, Version 1.2, Dierks & Rescorla - Standard Track, August 2008 (http://www.ietf.org/rfc/rfc5246.txt).

[RFC5639] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010

RFC5869] RFC 5869 - HMAC-based Extract-and-Expand Key Derivation Function (HKDF), IETF Trust and the persons identified as the document authors, May 2010 (http://www.ietf.org/rfc/rfc5869.txt).

[RFC6960] RFC 6960 - X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, June 2013 (https://www.ietf.org/rfc/rfc6960.txt)

RFC7027] RFC 7027 - Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), IETF Trust and the persons identified as the document authors, October 2013

[RFC7515] RFC 7515 - JSON Web Signature (JWS), IETF Trust and the persons identified as the document authors, May 2015 (http://www.ietf.org/rfc/rfc7515.txt).

RFC8446] RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3, IETF Trust and the persons identified as the document authors, August 2018 (http://www.ietf.org/rfc/rfc8446.txt).

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