Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1201-2022

zu

secunet konnektor 2.0.0, Version 5.1.2:2.0.0

der

secunet Security Networks 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-1201-2022 (*)

Gesundheitswesen: Konnektoren

secunet konnektor 2.0.0, Version 5.1.2:2.0.0

von	secunet Security Networks AG
PP-Konformität:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor, Version 1.6, BSI-CC-PP-0098-V3-2021-MA-01 vom 30.03.2022
Funktionalität:	PP konform plus produktspezifische Ergänzungen 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, AVA_VAN.3 und ALC_FLR.2

SOGIS
Recognition Agreement

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), 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.

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.

Common Criteria
Recognition Arrangement
Anerkennung nur für
Komponenten bis EAL 2
und ALC_FLR

Bonn, 9. September 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 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 und für Heimat
- 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 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 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 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).

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

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite https://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 und ALC_FLR 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 secunet konnektor 2.0.0, Version 5.1.2:2.0.0 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-1184-2022. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-1184-2022 wiederverwendet.

Die Evaluation des Produkts secunet konnektor 2.0.0, Version 5.1.2:2.0.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 12. August 2022 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller ist: secunet Security Networks AG.

Das Produkt wurde entwickelt von: secunet Security Networks AG.

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

[5] Information Technology Security Evaluation Facility

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 9. September 2022, ist gültig bis 08. September 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 secunet konnektor 2.0.0, Version 5.1.2:2.0.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[6] secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
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) ist ein Softwareprodukt, genannt Konnektor, bestehend aus dem Netzkonnektor und dem Anwendungskonnektor nach dem Protection Profile Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098 [8].

Der Netzkonnektor umfasst die Sicherheitsfunktionen einer Firewall und eines VPN-Clients, NTP-Servers Namens- (DNS) und DHCP-Dienstes. Er enthält auch die Grundfunktionen zum Aufbau sicherer TLS-Verbindungen zu anderen IT-Produkten.

Die Sicherheitsfunktionalität des Anwendungskonnektors umfasst die Signaturanwendung, die Verschlüsselung und Entschlüsselung von Dokumenten, den Kartenterminaldienst und den Chipkartendienst. Zusammen mit dem Netzkonnektor ermöglicht der Anwendungskonnektor zudem die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und Fachdiensten. Insbesondere setzt der Konnektor Kommunikationsprotokolle für die sichere Anbindung an das ePA-Aktensystem der Telematikinfrastruktur um. Der Konnektor wird als Einbox-Konnektor in Form einer komplett geschlossenen, passiv gekühlten Appliance umgesetzt.

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 3 mit Zusatz von ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6.2 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
Sicherheitsfunktionalität des Netzkonnektors als Teil des EVG	
VPN-Client	Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service (SIS) bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut, hierbei wird IKEv2 unterstützt.
Informationsflusskontrolle	Regelbasiert nutzen alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel. Nur Informationsflüsse, die vom Konnektor initiiert wurden sowie Informationsflüsse von Clientsystemen in Bestandsnetze dürfen den VPN-Tunnel in die Telematikinfrastruktur benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale TI-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen Netzen der Leistungserbringer betreffen, nutzen den VPN-Tunnel zum Sicheren Internet Service (SIS).
Dynamischer Paketfilter	Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird als Informationsflusskontrolle modelliert. Die Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt und können vom Administrator für den SIS verwaltet werden.
Netzdienste: Zeitsynchronisation	Der EVG führt bei bestehender Verbindung zur TI in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs am Gehäuse des Konnektors, u.a. auch für die Anzeige der Verbindung zur TI.
Netzdienste: Zertifikatsprüfung	Der EVG überprüft die Gültigkeit der Zertifikate, die für den Aufbau der VPN-Tunnel verwendet werden. Die erforderlichen Informationen zur Prüfung der Gerätezertifikate werden dem EVG in Form einer (signierten) Trust-service Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch mittels der aktuell gültigen TSL und CRL.
Stateful Packet Inspection	Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“. Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird.
Selbstschutz: Speicheraufbereitung	Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session-keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben mit Nullen. Der EVG speichert medizinische Daten nicht dauerhaft. Ausnahmen sind die Speicherung von Daten während ihrer Ver- und Entschlüsselung; auch diese werden sobald wie möglich nach ihrer Verwendung gelöscht.
Selbstschutz: Selbsttests	Der EVG bietet seinen Benutzern die Möglichkeit zur Integritätsprüfung. Es wird bei Programmstart eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) durch Verifikation von Signaturen durchgeführt. Dies wird durch eine sichere Bootkette umgesetzt. Die Selbsttest-Funktion (u.a. Secure Boot) kann nicht deaktiviert bzw. manipuliert werden. Im Falle einer Software-Aktualisierung wird dieselbe Bootkette durchlaufen. Das neue SW-Image wird vom Bootloader geprüft und geladen. Schlägt die Prüfung der Integrität fehl, so wird ein Neustart des EVG durchgeführt und anschließend wird das ursprüngliche SW-Image geladen.

Sicherheitsfunktionalität des EVG	Thema
Selbstschutz: Schutz von Geheimnissen, Seitenkanalresistenz	Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme. Dies gilt grundsätzlich für kryptographisches Schlüsselmaterial. Der private Authentisierungsschlüssel für das VPN wird bereits durch die gSMC-K und deren Resistenz gegen Seitenkanalangriffe geschützt. Der EVG verhindert darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll, etwa die session-keys der VPN-Verbindung oder zu schützende Daten der TI und der Bestandsnetze.
Selbstschutz: Sicherheits-Log	Der EVG führt ein Sicherheits-Log gemäß Konnektorspezifikation [13], [gemSpec_Kon].
Administration	Der EVG setzt Lokales und Remote Management um. Der Administrator muss autorisiert sein, bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf. Die Authentisierung erfolgt dabei durch den Netzkonnektor selbst. Zu den administrativen Tätigkeiten bzw. Wartungstätigkeiten gehören neben der Konfiguration des Konnektors u.a. die Verwaltung der Filterregeln für den dynamischen Paketfilter sowie das Aktivieren und Deaktivieren des VPN-Tunnels. Die Administration der Filterregeln für den dynamischen Paketfilter ist den Administratoren vorbehalten.
Software Update	Signierte Update-Pakete werden importiert und im Datenspeicher des EVG abgelegt. Sobald ein Update-Paket zur Verfügung steht signalisiert der TOE dass ein Software Update-Paket zur Verfügung steht. Der Administrator kann die Version des Update-Paketes prüfen und den Updateprozess anstoßen. Die Automatische Installation von Software Updates wird vom EVG nicht unterstützt. Im Falle einer Software-Aktualisierung wird der EVG neu gestartet und dieselbe Bootkette, wie in der Sicherheitsfunktion „Selbstschutz“ beschrieben, abgelaufen. Das neue Update-Paket wird vom Bootloader auf Integrität geprüft und bei erfolgreicher Prüfung geladen. Das alte Image wird vom EVG verworfen. Schlägt die Prüfung der Integrität fehl, so wird das Update-Paket verworfen und ein Neustart des EVG durchgeführt mit dem das ursprüngliche SW Image geladen wird. Durch die Prüfung des Update-Pakets analog zum regulären Boot-Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können.
Kryptographische Basisdienste	Der Konnektor implementiert Kryptographische Basisdienste für den Aufbau von sicheren VPN-Verbindungen zu den VPN-Konzentratoren der TI und des SIS.
TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen	Der Netzkonnektor stellt dem Anwendungskonnektor die Dienste zum Aufbau eines TLS-Kanals zur Verfügung. TLS wird auch zur Absicherung der Administratorschnittstelle verwendet. Die kryptographischen Basisdienste für TLS des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des TLS-Kanals). Zertifikate die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen, werden vom Netzkonnektor entsprechend den Anforderungen in der Konnektorspezifikation [13], [gemSpec_Kon], interpretiert. Der EVG prüft insbesondere, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist enthalten ist. Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen werden X.509-Zertifikate verwendet. Entsprechende Zertifikate für das Clientsystem können vom EVG erzeugt werden. Der EVG bietet dem Administrator eine sichere Schnittstelle zum exportieren dieser X.509-Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel. Zertifikate für

Sicherheitsfunktionalität des EVG	Thema
	Clientsysteme können auch vom EVG über die gesicherte Management-Schnittstelle durch den Administrator importiert werden, um ggf. benötigte Betriebszustände wiederherzustellen. Die TLS-Verbindungen werden vom Anwendungskonnektor gemanagt und je nach Anwendungsfall eingerichtet.
Sicherheitsfunktionalität des Anwendungskonnektors als Teil des EVG	
Identifikation und Authentisierung	Der Anwendungskonnektor setzt unterschiedliche Mechanismen zur Identifikation und Authentisierung von Benutzern um. Die Management-Schnittstelle des Konnektors ist durch Passworteingabe vor unautorisiertem Zugriff geschützt. Dabei gelten die folgenden Anforderungen nach Konnektorspezifikation [13], [gemSpec_Kon], TIP1-A_4808, an die Administratorpasswörter. Im Rahmen des Pairing eines eHealth-Kartenterminals generiert der Konnektor das „pairing secret“ mit hinreichend großer Entropie. Wird ein angeschlossenes Kartenterminal für Stapelsignaturen verwendet, so fordert der Konnektor die Übertragung der DTBS über einen sicheren Kanal der mittels card-to-card authentication mit dem HBA ausgehandelt wird.
Zugriffsberechtigungsdienst	Der Zugriffsberechtigungsdienst (oder Zugriffskontrolldienst) ist ein interner Dienst des Konnektors der automatisch bei Aufruf einer Operation des Konnektors durch das Clientsystem umgesetzt wird. Durch den Zugriffskontrolldienst wird eine Prüfung auf Zugriffsberechtigung für die an-geforderten Ressourcen durchgeführt. Die erlaubten Zugriffsmöglichkeiten werden über ein Informationsmodell (kurz Infomodell) definiert. Durch das Infomodell werden Mandanten definiert und Clientsysteme sowie die vom Konnektor verwalteten externen Ressourcen (Kartenterminal mit Slots, Arbeitsplatz, SMC-Bs) zugeordnet. Die entsprechenden Zuordnungen werden durch einen Administrator eingestellt und beinhalten die erlaubten Zugriffswege vom Clientsystem über Arbeitsplatz zum Kartenterminal und dessen Slots.
Kartenterminaldienst	Die Aufgabe des Kartenterminaldienstes ist das Management aller vom Konnektor adressierbaren Kartenterminals (KT). Dabei kapselt der Kartenterminaldienst die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule. Über den Kartenterminaldienst können TLS-Kanäle zu den KTs auf- und abgebaut, sowie SICCT-Kommandos gesendet und empfangen werden. Der Anwendungskonnektor kommuniziert mit den konfigurierten eHealth-Kartenterminals über TLS-Kanäle. Der Netzkonnektor stellt diese Kommunikationskanäle kontrolliert dem Anwendungskonnektor zur Verfügung. Informationen über die Arbeitsplatzkonfiguration eines angeschlossenen Kartenterminals können vom Kartenterminaldienst ausgegeben werden. Nur der Administrator darf diese Daten auch verändern.
Kartendienst	Die eHealth-Kartenterminals unter der Steuerung des Anwendungskonnektors können verschiedene Chipkarten (KVK, eGK, SMC-B und HBA) aufnehmen. Die in den eHealth-Kartenterminals eines Arbeitsplatzes gesteckten Chipkarten mit ihren logischen Kanälen bilden einen dynamischen Kontext (s. Konnektorspezifikation [13], [gemSpec_Kon]). Die Identifikation dieser Chipkarten erfolgt durch Kartenhandles. Der EVG stellt Sicherheitsfunktionen des Chipkartendienstes anderen Diensten, dem Clientsystem oder den Fachmodulen, bereit. Dazu gehören der Aufbau und die Verwaltung logischer Kanäle und die Kommunikation mit der Karte via Chipkartenkommandos. Der Chipkartendienst regelt dabei den

Sicherheitsfunktionalität des EVG	Thema
	Zugriff auf die Chipkarten für die verschiedenen Dienste und Anwender. Zudem wird durch den Chipkartendienst die lokale und entfernte PIN-Eingabe an den Kartenterminals umgesetzt und die unterschiedlichen Anforderungen an lokale und entfernte PIN-Eingabe und der damit verbundene Umgang mit den so genannten Authentisierungsverifikationsdaten (VAD) geregelt.
Signaturdienst	Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten und Prüfen von Dokumentensignaturen an. Die zu signierenden oder zu prüfenden Daten können vom Konnektor bei Bedarf entsprechend der referenzierten NFDM Signaturrichtlinie behandelt werden. Der Signaturdienst unterstützt nicht-qualifizierte elektronische Signaturen (nonQES) sowie qualifizierte elektronische Signaturen (QES), die mit Hilfe der vom Chipkartendienst verwalteten Chipkarten erzeugt werden. Der Signaturdienst unterstützt die folgenden Signaturformate für nonQES und QES: • XAdES für XML Dokumente (Nur QES mit NFDM-Signaturrichtlinie), • CAdES für XML, PDF/A, Text und TIFF Dokumente • PAdES für PDF/A Dokumente. Darüber hinaus werden für nonQES die folgenden Signaturformate unterstützt: • CAdES für Binärdokumente Zudem wird für nonQES und QES PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 unterstützt. Das Prüfen von Dokumentensignaturen erfolgt anhand von Zertifikaten. Bei Feststellung ungültig erzeugter Signaturen wird der Benutzer entsprechend durch eine Warnmeldung benachrichtigt. Der Benutzer des Clientsystems muss seine Signatur-PIN an einem angeschlossenen eHealth-Kartenterminal eingeben.
Software-Update	Signierte Update-Pakete werden importiert und im Datenspeicher des EVG abgelegt. Sobald ein Update-Paket zur Verfügung steht, signalisiert der TOE, dass ein Software Update zur Verfügung steht. Der Administrator kann die Version des Update-Paketes prüfen und den Updateprozess anstoßen. Es können nur Update-Pakete erfolgreich installiert werden, deren Signatur erfolgreich geprüft wurde. Die Firmwaregruppe des Updates muss gleich oder höher der gegenwärtig installierten Firmwaregruppe sein. Der Updateprozess verhindert, dass manipulierte Update-Pakete eingespielt werden. Fachmodule können nur im Rahmen von Software-Updates des Konnektors aktualisiert oder eingebracht werden.
Verschlüsselungsdienst	Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an. Der Verschlüsselungsdienst bietet für XML, PDF/A, Text, TIFF und Binärdaten die hybride Ver- und Entschlüsselung nach dem CMS-Standard [12] [RFC5652] bzw. die symmetrische Ver- und Entschlüsselung mittels AES-GCM an. Zudem wird für XML-Dokumente die hybride Ver- und Entschlüsselung nach [12] [XMLEnc] unterstützt. Dem Konnektor werden durch das Clientsystem die zu verschlüsselnden und zu entschlüsselnden Dokumente übergeben und beim Verschlüsseln eines Dokuments die vorgeschlagenen Empfänger des Dokuments angegeben. Vor dem Verschlüsseln eines Dokuments wird die Gültigkeit der zu benutzenden

Sicherheitsfunktionalität des EVG	Thema
	Verschlüsselungszertifikate geprüft.
TLS-Kanäle	Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung. Die Verwaltung von TLS-Kanälen wird duch den Anwendungskonnektor durchgeführt. Der Anwendungskonnektor initiiert dabei den Auf- und Abbau der TLS-Kanäle und stellt den Endpunkt für das Senden und Empfangen der Nutzdaten dar. Für das VSDM Fachmodul wird zudem TLS Session Resumption unterstützt. Der Administrator kann konfigurieren, ob für Verbindungen zum Clientsystem TLS-Kanäle verwendet werden müssen (ANCL_TLS_MANDATORY, ANCL_CAUT_MANDATORY) und einen zertifikats oder passwortbasierten Authentisierungsmechanismus (ANCL_CAUT_MODE) festlegen. Für den Dienstverzeichnisdienst kann explizit die verpflichtende Nutzung von TLS deaktiviert werden (ANCL_DVD_OPEN). TLS-Kanäle werden unter anderem für die Kommunikation mit Fachdiensten, mit dem zentralen Verzeichnisdienst, dem KSR, dem TSL-Dienst, bei ANCL_TLS_MANDATORY = Enabled mit den Clientsystemen im LAN und mit den angebundenen eHealth-Kartenterminals verwendet.
Sicherer Datenspeicher	Der Konnektor stellt einen Datenspeicher zur Verfügung, in welchem er alle sicherheitskritischen, veränderlichen Daten dauerhaft speichert, die für seinen Betrieb relevant sind. Dieser Datenspeicher sichert die Vertraulichkeit der in ihm hinterlegten Daten bzw. der aus ihm entnommenen Daten. Der Konnektor stellt den in ihm laufenden Fachmodulen ebenfalls eine Nutzung dieses Datenspeichers für deren sensible Daten zur Verfügung.
Fachmodul VSDM	Das Fachmodul Versicherten Stammdaten Management (VSDM) ist fester Bestandteil des EVG und ermöglicht es, Versichertenstammdaten einer eGK zu lesen, zu schreiben oder um neue Einträge zu ergänzen. Die eGK wird dabei über den Kartenterminaldienst und den Kartendienst angesprochen. Das VSDM-Fachmodul kann über die Management-Oberfläche administriert werden.
Sicherheitsmanagement	Der Konnektor verwaltet verschiedene Rollen, wie Administrator, Clientsystem, Kartenterminals und Chipkarten. Auf die Management-Schnittstelle hat nur ein autorisierter Administrator Zugriff. Dieser kann zum Beispiel Kartenterminals managen, Arbeitsplätze konfigurieren, Sicherheitsrichtlinien und TLS-Kanäle verwalten. Dazu gehört auch das Verwalten von Software Updates für den EVG und angebundene Kartenterminals, Verwalten von Zertifikaten und Durchführen eines Werksresets. Insbesondere kann der Administrator die Online-Anbindung des Konnektors im Netz des Leistungserbringers konfigurieren (MGM_LU_ONLINE) und die QES-Funktionalität des Signaturdienstes de/-aktivieren (MGM_LU_SAK). Die öffentlichen Schlüssel der CVC root CA sind in der gSMC-K gespeichert und können nur durch das CMS System der gSMC-K gelöscht werden. Über Cross-CVC-Zertifikate können durch den Anwendungskonnektor aber weitere öffentliche Schlüssel der CVC root CA eingebracht werden.
Schutz der TSF	Der Konnektor kann die für QES und nonQES benötigten Zertifikate interpretieren, sowie Verschlüsselungszertifikat und CV-Zertifikate. Zudem werden Informationen gültiger TSL- und CRL-Listen in die Prüfungen einbezogen sowie BNetzA-VL bzw. die entsprechenden Hashwerte. Die Zulässigkeit importierter zu signierender bzw. zu prüfender signierten Daten wird bei Bedarf gemäß NFDM-Signaturrichtlinie geprüft. Der Konnektor setzt die in der Konnektorspezifikation [13], [gemSpec_Kon], TAB_KON_503, definierten Fehlbetriebszustände um (Error Condition). Wird ein

Sicherheitsfunktionalität des EVG	Thema
	sicherheitsrelevanter Betriebszustand erreicht, schränkt der Konnektor seine Funktionalität gemäß Konnektorspezifikation [13], [gemSpec_Kon], TAB_KON_504, ein. Vor der regulären Kommunikation mit einem eHealth-Kartenterminal wird geprüft, ob dieses gepairt ist und im Infomodell des Konnektors korrekt zugeordnet wurde. Ebenso werden gesteckte Chipkarten identifiziert und auf Gültigkeit geprüft. Bei entfernter PIN-Eingabe wird geprüft ob Kartenterminal und HBA für diesen Verwendungsfall zugelassen sind, Der Konnektor führt beim Anlauf und regelmäßig während des Normalbetriebs Selbsttests durch. Neben Selbsttests im Rahmen des sicheren Start-Up-Prozesses wird insbesondere auch die Implementierung der Trusted Channels (IPSec und TLS) beim Hochfahren getestet. Im Normalbetrieb werden regelmäßig die Funktionalitäten AES und TLS getestet. Durch den sicheren Start-Up-Prozess wird die Integrität des TOEs auf einen sicheren Vertrauensanker im BIOS zurückgeführt. Durch Neustart des Konnektors können die damit verbundenen Prüfungen durch einen Benutzer jederzeit wiederholt werden. Die vom Anwendungskonnektor erzeugten Protokolleinträge des Sicherheitsprotokolls werden mit einem zuverlässigen Zeitstempel versehen. Der Anwendungskonnektor greift dabei auf die Echtzeituhr zurück, die in regelmäßigen Abständen und auf Anforderung des Administrators mit einem vertrauenswürdigen Zeitdienst synchronisiert wird.
Sicherheitsprotokollierung	Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation [13] [gemSpec_Kon]. Nur der Administrator kann Protokolleinträge einsehen. Protokolleinträge können nicht verändert werden und nicht explizit gelöscht werden. Ältere Einträge werden rollierend überschrieben.
VAU-Kanal	Der Konnektor unterstützt das ePA Fachmodul mit dem Aufbau einer sicheren Verbindung zur Vertrauenswürdigen Ausführungsumgebung (VAU) gemäß VAU-Kommunikationsprotokoll. Dabei wird ein sicherer Kanal auf HTTP-Anwendungsschicht zwischen dem Client und der VAU (Server) aufgebaut.
SGD-Kanal (Schlüsselgenerierungsdienst)	Der Konnektor unterstützt das ePA-Fachmodul bei der Nutzung der Schlüsselableitungsfunktionalität im Zusammenhang der ePA Fachanwendung. Der Gesamtablauf der Schlüsselableitungsfunktionalität für den Konnektor als Client ist aufgeteilt zwischen Basiskonnektor (als Teil des Anwendungskonektors) und Fachmodul. Die kryptographischen Vorgaben (u.a. Durchführung des ECDH, Schlüsselerzeugung, Ver- und Entschlüsselung, Signaturerzeugung und -prüfung) werden dabei durch den Konnektor realisiert.

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 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in den Kapiteln 3.2, 3.3 und 3.4 dar.

Dieses Zertifikat umfasst die in Kapitel 8 beschriebene Konfiguration des EVG.

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:

secunet konnektor 2.0.0, Version 5.1.2:2.0.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifikator	Version	Auslieferungsart
1.	HW	secunet konnektor 2.0.0 Hardware für Einbox-Konnektor (EBK) (nicht Teil des EVG)	Hardware Version: 2.0.0 (EBK) BIOS FW Version: CSASR007, CSASR009, CSASR011	Das Gerät wird über eine sichere Lieferkette dem Endkunden zugestellt.
2.	HW	gSMC-Ks (nicht Teil des EVG)	Kartentypen[7]: ● STARCOS 3.6 Health SMCK R1 ● TCOS Security Module Card – K Version 2.0 Release 1 ● STARCOS 3.7 gSMC-K R1 ● TCOS Security Module Card – K Version 2.0 Release 2	Die gSMC-Ks sind in der Konnektor-Hardware verbaut.
3.	SW	secunet konnektor 2.0.0 Firmware	EVG-Version:5.1.2:2.0.0 bestehend aus: Netzkonnektor-Version: 5.1.2[8] Anwendungskonnektor-Version: 5.1.2	Die Software wird im Zuge der Fertigung auf die Hardware gebracht und über eine sichere Lieferkette ausgeliefert. Es besteht zusätzlich die Möglichkeit, dass die Software als Software-Update-Paket über KSR verteilt werden kann.
4.	SW	AMTS, NFDM und ePA Fachmodul Firmware (nicht Teil des EVG)	NFDM-Fachmodul: secunet Fachmodul NFDM 5.1.1 AMTS-Fachmodul: secunet Fachmodul AMTS 5.1.1 ePA-Fachmodul: secunet Fachmodul ePA 5.1.1	Die Fachmodule sind integraler Bestandteil des Anwendungskonnektor-Image.

[7] Je Konnektor sind immer identische gSMC-Ks eines der hier genannten Kartentypen verbaut, die anhand der Identifikationsnummer (ICCSN) ermitteln werden können, siehe Handbuch [10] [a].

[8] Die Angabe gilt als Gesamtversion der Firmware, d.h. inkludiert die Anwendungskonnektor-Version

Nr	Typ	Identifikator	Version	Auslieferungsart
5.	DOC	Zugehörige Handbücher	secunet(konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Bedienungsanleitung, Für Administratoren und Benutzer, Version 6.1, 09.06.2022, secunet Security Networks AG SHA256: aff8fc95cff872221922e2ae94645fe3db3b5a48b48cee1fb43e2d3537cea9cf Errata der Bedienungsanleitung Version 6.1 vom 09.06.2022, Version 1.0, 27.06.2022, secunet Security Networks AG SHA256: 48e132263e912a0848e03377c0f395582f03ff4f8bd87c6342e334836894576f	Die Handbücher können auf der Herstellerwebseite heruntergeladen werden.
6.	DOC		secunet(konnektor v2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 1.8, 31.10.2019 SHA256: 5D7B1F22E54EC1C59D1E74A3EDC0D8207C919576F54B9EBF7BF360B9D39E5F8E	
7.	DOC		Konnektor Management API-Dokumentation, eHealth Experts GmbH, Version 5.0.0, 11.05.2022 SHA256: 04a4a5718cb077fc4fe7fe6d1a9afa27d04c2d66637591df21b6e57090526a82	Die REST-API Spezifikation der Management-Schnitt-stelle wird im Handbuch [10] [a], Kap. 8, erwähnt und nur auf Anfrage durch den Hersteller gezielt ausgeliefert.
8.	DOC		Security Guidance Fachmodulentwicklung; eHealth Experts GmbH; v.1.5; 19.04.2021 SHA256: 8CF0B092EC51D3CAC35C8A7B36FFB810CD4F618309B79281295153C2FEF61F77	Die Security Guidance Fachmodulentwicklung wird nur intern den Fachmodul-Entwicklern zur Verfügung gestellt.

Tabelle 2: Auslieferungsumfang des EVG

Die sichere Lieferkette wird in [9] beschrieben. Die Anweisungen an den Nutzer, wie die Einhaltung der sicheren Lieferkette überprüft werden kann, sind in [10] [b] beschrieben.

Das Gerät, welches den EVG beinhaltet, ist in einem Gehäuse untergebracht, und verfügt über die Hardwareanschlüsse, die für den Betrieb des EVG notwendig sind. Die gSMC-Ks befinden sich ebenfalls in diesem Gehäuse.

Die Version des EVG kann über die grafische Benutzeroberfläche ermittelt werden. Eine Beschreibung dazu findet sich in [10] [a], Kapitel 9.5.6. Im Bereich “Version” werden Produktdaten und Versionsangaben angezeigt, wie zum Beispiel Firmware Version (EVG Version), die Hardware Version der unterliegenden Hardware sowie die Seriennummer

des Geräts. Mit “Details” können weitere Einzelheiten zum System angezeigt werden, wie zum Beispiel die Version der Anwendungskonnektor-Komponente.

Die im Konnektor verbauten gSMC-Ks können anhand der Identifikationsnummer (ICCSN) ermittelt werden, siehe [10] [a], Kapitel 9.3.1. Die ICCSN der Karte besteht aus 20 Stellen. Die elfte Stelle der ICCSN gibt dabei an, welcher Typ der gSMC-Ks im secunet konnektor 2.0.0 verbaut ist, siehe [10] [a], Tabelle 19 und Kapitel 9.3.1

3. Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Die durchgesetzte Sicherheitspolitik ist durch eine ausgewählte Menge an SFRs definiert und wird vom EVG umgesetzt. Der EVG implementiert logische Sicherheitsfunktionalität, um schützenswerte Daten, die vom EVG gespeichert und verarbeitet werden, während des Betriebs in einer sicheren Einsatzumgebung zu schützen. So erhält der EVG die Integrität gespeicherter Daten durch seine Möglichkeiten zur Konfiguration, Speicherzugriff und seiner umgesetzten Sicherheitsfunktionen. Weitere Details hierzu können dem Security Target, [6], Kap. 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. Insbesondere sind die folgenden Punkte relevant:

- OE.NK.CS: Korrekte Nutzung des Konnektors durch Clientsysteme und andere aktive Komponenten im LAN
- OE.NK.Admin_EVG: Sichere Administration des Netzkonnektors
- OE.NK.phys_Schutz: Physischer Schutz des EVG
- OE.NK.Betrieb_CS: Sicherer Betrieb der Clientsysteme
- OE.AK.sichere_TI: Sichere Telematikinfrastruktur-Plattform
- OE.AK.Admin_EVG: Sichere Administration des Anwendungskonnektors
- OE.AK.Plattform: Sichere Plattform
- OE.AK.PKI: PKI für Signaturdienste, Verschlüsselung und technische Komponenten
- OE.AK.Clientsystem: Sichere Clientsysteme
- OE.AK.SW-Update: Prozesse für sicheres Software-Update

Details und weitere Punkte finden sich in den Sicherheitsvorgaben [6], Kapitel 4.3 und 4.4.

5. Informationen zur Architektur

Der EVG ist ein Softwareprodukt, das auf dem Betriebssystem Linux basiert. Dieser Abschnitt liefert eine Übersicht über die Subsysteme des EVG und die entsprechenden TSF, die Gegenstand dieser Evaluierung waren. Die Sicherheitsfunktionen des EVG sind:

Netzkonnektor:

VPN-Client, Dynamischer Paketfilter mit zustandsgesteuerter Filterung, Netzdienste (Zeitsynchronisation und Zertifikatsprüfung), Stateful Packet Inspection, Selbstschutz (Speicheraufbereitung, Selbsttests, Schutz von Geheimnissen und Seitenkanalresistenz, Sicherheits-Log), Administration (Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung und Software Update), Kryptographische Basisdienste und TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen.

Anwendungskonnektor:

Identifikation und Authentisierung, Zugriffsberechtigungsdienst, Kartenterminaldienst, Kartendienst, Signaturdienst, Software-Update, Verschlüsselungsdienst, TLS-Kanäle, Sicherer Datenspeicher, Fachmodul VSDM, Sicherheitsmanagement, Schutz der TSF, Sicherheitsprotokollierung, VAU-Kanal und SGD-Kanal.

Entsprechend dem TOE Design werden diese Sicherheitsfunktionen von folgenden Subsystemen umgesetzt:

- Konnektor-Basissystem: Dieses Subsystem umfasst u.a. den Systemstart für den Netzkonnektor, die Schnittstelle zum Anwendungskonnektor, das Starten/Stoppen von Netzwerkdiensten, die Konfiguration von Netzwerkschnittstellen, die LED-Steuerung, den Kartenleser, DNS, NTP, DHCP-Server, die Laufzeitumgebung für den Anwendungskonnektor, Logging u.w.
- Subsystem VPN: Dieses Subsystem umfasst u.a. die Initialisierung von neuen IPSec-Verbindungen, die Ver- und Entschlüsselung von IPSec-Paketen, u.w.
- TLS-Basis Subsystem: Dieses Subsystem dient u.a. dem Aufbau einer authentisierten und sicheren Verbindung über TLS.
- Konnektormanagement Subsystem: Über dieses Subsystem wird die gesamte Funktion und Konfiguration des Konnektors gesteuert.
- Laufzeitumgebung Subsystem: Dieses Subsystem fasst Basisfunktionalität zusammen, die von anderen Subsystemen benötigt werden.
- Fachmodul-VSDM: Dieses Subsystem setzt die Fachanwendung Versichertenstammdatenmanagement (VSDM) um. Es ermöglicht das Auslesen und Aktualisieren von Versichertenstammdaten einer elektronischen Gesundheitskarte (eGK) sowie das Auslesen des Datensatzes einer Krankenversichertenkarte (KVK).
- Subsystem Anwendungskonnektor PTV3: Dieses Subsystem umfasst u.a. den Zugriffsberechtigungsdienst, den Dokumentenvalidierungsdienst, den Dienstverzeichnisdienst, den Kartenterminaldienst, den Kartendienst, den Verschlüsselungsdienst, den Signaturdienst, den Zertifikatsdienst, den TLS-Dienst für Fachmodule, den Protokollierungsdienst, den Selbsttest-Dienst, den Konnektorstatusdienst, u.w.
- Subsystem Anwendungskonnektor PTV4: Dieses Subsystem umfasst, die zur Kommunikation mit dem ePA Aktensystem benötigten Module des VAU- und SGD-Clients.
- Subsystem Anwendungskonnektor PTV5: Dieses Subsystem stellt eine Erweiterung bestehender Module dar, u.a. die Implementierung der Komfortsignatur, für TLS die ECC-Migration und die Nutzung von Software-Serverzertifikaten, u.w.

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

Zur Bestätigung aller Sicherheitsfunktionen des EVG wurden folgende Methoden angewendet:

- automatisiertes Testen aller TSFI
- manuelles Testen aller TSFI
- Sourcecode-Reviews
- Netzwerktests einschließlich gezielter Tests der Protokolle IPsec und TLS

Für das Testen durch die Prüfstelle wurden sowohl die Ausprägungen “Release” als auch “Extended Release” verwendet. Diese Ausprägungen sind konsistent mit den Angaben im Security Target

In den Fällen, bei denen die Tests nicht an der finalen Version, sondern an anderen Versionen durchgeführt wurden, wurde eine Analyse der Änderungen am EVG zwischen getesteter und finaler Version anhand der bereitgestellten Beschreibungen des Herstellers und insbesondere des Source-Codes durchgeführt. Dabei konnte festgestellt werden, dass eine Wiederholung der Tests an der finalen EVG-Version nicht notwendig ist, da die jeweils getestete Sicherheitsfunktion sich nicht geändert hat und durch die Änderungen am EVG nicht beeinflusst wird. Die an den jeweiligen Vorversionen erhaltenen Testergebnisse sind somit vollständig auf die finale EVG-Version 5.1.2 übertragbar.

Bei Tests und Schwachstellenanalyse wurde systematisch das Angriffspotential “Enhanced-Basic” (AVA_VAN.3) unterstellt.

Die tatsächlichen Ergebnisse des Testens entsprachen den erwarteten und spezifizierten Ergebnissen.

Bei der Schwachstellenanalyse wurden zuerst veröffentlichte Schwachstellen auf ihre Relevanz in der Einsatzumgebung des EVG untersucht und ggf. weiteren Tests und Analysen unterzogen.

Es wurde unter Berücksichtigung des unterstellten Angriffsniveau keine ausnutzbare Schwachstelle identifiziert.

Herstellertests

Der Hersteller hat zwei verschiedene Testumgebungen bereitgestellt, die im Folgenden beschrieben werden. Die meisten Tests wurden dabei an der Testumgebung „ANKE“ durchgeführt.

Testumgebung ANKE

Die Test-Engine und die entsprechenden Test-Module sind in der Programmiersprache Java implementiert und verwenden die Java-Laufzeitumgebung (JRE) inklusive deren Netzwerkfunktionalität.

Die Testlogik ist in einzelnen Test-Modulen enthalten, die für die jeweiligen Testfälle mit unterschiedlichen Parametern aufgerufen und kombiniert werden können. Dabei können Test-Module für beliebige Testfälle wiederverwendet werden. Das Testergebnis einzelner Testfälle wird durch separate Evaluator-Module bewertet, die ebenfalls bei der Zusammenstellung der einzelnen Testfälle mehrfach verwendet werden.

Die Schnittstellen werden durch Test-Module getestet, die in der Testumgebung des Herstellers eingebaut sind. Jedes Test-Modul testet dabei eine definierte Funktionalität.

Testumgebung NWTU

Der Hersteller hat neben der oben beschriebenen Testumgebung eine weitere Testumgebung für die Ausführung bestimmter Testfälle bereitgestellt. Diese alternative Netzwerktestumgebung wurde für Testszenarien, die auf das Testen von Netzwerk-funktionen abzielen und nicht ohne erheblichen Aufwand mit der anderen Testumgebung umgesetzt werden können, entwickelt.

Die Testfälle sind als Unix Shell Scripts implementiert. Nach jeder Testausführung wird eine Logdatei erstellt, die das jeweilige Testergebnis PASSED, FAILED oder ABORTED enthält.

Testansatz des Herstellers

Der Testansatz des Herstellers ist das direkte Testen der SFRs. Diese SFRs sind wiederum auf die sicherheitsrelevanten Schnittstellen (TSFIs) des EVGs abgebildet. Zusätzlich wurden weitere Testfälle durch den Hersteller implementiert, die nicht direkt auf Anforderungen der gematik Spezifikation zurückzuführen sind, aber Sicherheitsfunktionen adressieren, die in den Sicherheitsvorgaben [6] definiert sind. Alle relevanten Testfälle wurden auf SFRs abgebildet und jedes SFR ist von mindestens einem Testfall abgedeckt. In Einzelfällen wurde begründet, wie die korrekte Umsetzung der Sicherheitsfunktion bereits auf andere Weise verifiziert wird (z. B. durch Source Code Analyse). Um sicherzustellen, dass die Sicherheitsfunktionalität, wie sie in der Funktionalen Spezifikation beschrieben ist, vollständig durch Testfälle abgedeckt wird, hat der Hersteller eine Abdeckungsanalyse aller SFRs durch TSFIs und umgekehrt durchgeführt. Jedes TSFI wird durch Testfälle abgedeckt.

Testergebnisse

Es wurden keine Abweichungen zwischen erwartetem und tatsächlichem Verhalten des EVG festgestellt.

Unabhängige Tests der Prüfstelle

Die unabhängigen Evaluatortests wurden mit den Testumgebungen des Herstellers durchgeführt. Zudem kamen weitere Testwerkzeuge der Prüfstelle zum Einsatz, z. B. Tools zum Versenden und Empfangen von REST-Befehlen.

Für Testzwecke wurde der Prüfstelle die sogenannte "Extended Release" Variante des EVG zur Verfügung gestellt. Dadurch wurden Untersuchungen des EVG insbesondere für den AVA-Aspekt vereinfacht und zum Teil überhaupt erst möglich gemacht (z. B. durch Zugriff auf das Betriebssystem).

Die Extended-Release-Variante soll dabei neben den nötigen Anpassungen möglichst gering von der finalen Produktversion abweichen. Die Unterschiede zwischen EVG und Extended-Release-Variante wurden im Rahmen der Evaluierung untersucht und dabei konnte festgestellt werden, dass diese Unterschiede keinen Einfluss auf die damit erhaltenen Testergebnisse haben, insbesondere nicht auf die funktionalen Tests.

Weiterhin wurden alle automatisierten Testfälle der Herstellertestumgebung wiederholt.

Testergebnisse

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen festgestellt.

Penetrationstests der Prüfstelle

Die Konfiguration des EVG, die von dieser Evaluierung abgedeckt ist, wurde getestet.

Testergebnisse

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnisse festgestellt. Es war kein Angriffsszenario, welches einen Angreifer mit dem Angriffspotential „Enhanced-Basic“ voraussetzt, in der Betriebsumgebung, wie sie in den Sicherheitsvorgaben [6] definiert ist, erfolgreich durchführbar. Diese gilt unter der Annahme, dass alle Maßnahmen die vom Hersteller an den sicheren Betrieb gestellt sind auch umgesetzt werden.

8. Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf auf die Konfiguration „Einbox-Lösung“ als einzige Konfiguration des EVG (siehe [6], Kapitel 1.3).

Der Administrator kann über die Benutzeroberfläche die Version des EVG auslesen.

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 für die Komponenten bis zur Vertrauenswürdigkeitsstufe 5 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 3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die zusätzlichen Komponenten ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-1184-2022darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden.

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor, Version 1.6, BSI-CC-PP-0098-V3-2021-MA-01 vom 30.03.2022 [8]

- Funktionalität: PP konform plus produktspezifische Ergänzungen
  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, AVA_VAN.3 und ALC_FLR.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 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	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit	Anwendungsstandard	Kommentar
1.	Authentizität	RSA Verifikation von Signaturen für VPN und TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec_Krypt] Kap. 3.3.1 und Kap. 3.3.2	FPT_TDC.1/NK.Zert FPT_TDC.1/ NK.TLS.Zert
2.		ECDSA Verifikation von Signaturen für TLS ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen Kurven für brainpoolP256r1 ([RFC5639])	[gemSpec_Krypt] Kap. 3.3.1 und Kap. 3.3.2	FPT_TDC.1/ NK.TLS.Zert
3.		ECDSA Verifikation von Signaturen für VPN ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der Verwendeten elliptischen Kurven für brainpoolP256r1 ([RFC5639])	[gemSpec Krypt] Kap. 3.3.1 und Kap. 5.5	FPT_TDC.1/NK.Zert
4.		ECDSA Verifikation von Signaturen für VAU Protokoll ecdsa-with-Sha256 (OID 1.2.840.10045.4.3.2)	[gemSpec_Krypt], Kap. 6 (VAU) [TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256) Siehe Abwei-	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 6	FPT_TDC.1/SGDVAU

			chungen: [14], Kap. 4			
5.		ECDSA Signatur Erzeugung mit Unterstützung der SMC-B oder eGK und Verifikation für den SGD Klient ecdsa-with-Sha256 (OID 1.2.840.10045.4.3.2)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256) Siehe Abweichungen: [14], Kap. 4	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 3.15 (SGD)	FPT_TDC.1/SGDVAU FCS_COP.1.1/SGD.Auth Anmerkung: Im SGD Protokoll findet nur Authentifizierung und keine Authentisierung statt, da der zu signierende Inhalt vom SGD-Client gewählt wird oder bekannt ist. Im VAU Protokoll Authentisiert sich der Client durch die Signatur über die „VAUServerHelloData“.
6.		Verifikation von Signaturen der TSL mit RSASSA-PSS	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA) [RFC-6931] (XMLDSig)	2048 Bit	[gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/ NK.TLS.Zert FPT_TDC.1/AK
7.		Verifikation von Signaturen der CRL mit RSASSA-PKCS1-v1_5 sha256WithRSAEncryption	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/ NK.TLS.Zert FPT_TDC.1/AK
8.		Verifikation von Signaturen der BNetzA-VL RSASSA-PSS mit Hash Funktion SHA-{256, 512} und ECDSA mit Hash Funktion SHA-{256,384,512}	[RFC 8017] (PKCS#1) [TR-03111] (ECDSA) [FIPS 180-4] (SHA)	2048 - 8192 Bit für RSA Für ECDSA: Schlüssellänge entsprechend der verwendeten elliptischen Kurven brainpoolP{256,384,512}r1 ([RFC7027]) NIST P-{256,384,521} ([FIPS186-4]) FRP256v1 [ANSSI-0241]	[gemSpec_PKI], Kap. 8.5.2 [ETSI_TS_119_612]	FPT_TDC.1/AK
9.		Verifikation von Signaturen der TSL und CRL mit ECDSA	[TR-03111] ECDSA [RFC-5639] brainpool	Schlüssellänge entsprechend der verwendeten	[gemSpec_Krypt], Kap. 5.3	FPT_TDC.1/NK.Zert FPT_TDC.1/ NK.TLS.Zert

		ecdsa-with-SHA256	[FIPS 180-4] (SHA-256)	elliptischen Kurve brainpoolP256 r1 ([RFC5639])		FPT_TDC.1/AK
10.	Authenti-sierung	RSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für VPN und TLS sha256withRSAEncr yption (OID 1.2.840.113549.1.1.1 1) sha384withRSAEncr yption (OID 1.2.840.113549.1.1.1 2) (für TLS) sha512withRSAEncr yption (OID 1.2.840.113549.1.1.1 3) (für TLS)	[RFC-8017] (RSASSA-PKCS1-v1_5) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec _Krypt], Kap. 3.3.1	FCS_COP.1/NK.Auth FCS_COP.1/ NK.TLS.Auth
11.		ECDSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für TLS ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256 r1 ([RFC5639])	[gemSpec _Krypt], Kap. 3.3.2	FCS_COP.1/ NK.TLS.Auth
12.		ECDSA und RSA Signatur Erzeugung mit Softwarezertifikat für TLS ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) sha256withRSAEncr yption (OID 1.2.840.113549.1.1.1 1)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256) [RFC-8017] (RSASSA-PKCS1-v1_5)	RSA: 2048 Bit ECDSA: Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256 r1 ([RFC5639])	[gemSpec _Krypt], Kap. 3.3.2	FCS_COP.1/ NK.TLS.Auth FCS_CKM.1.1/NK.Zert
13.		ECDSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für VPN ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256)	Schlüssel-länge entsprechend der verwendeten el-liptischen Kurve brainoolP256r 1 ([RFC5639])	[gemSpec _Krypt], Kap. 3.3.1 und 5.5	FCS_COP.1/NK.Auth
14.		ECDSA Signatur Erzeugung mit Unterstützung der SMC-B oder eGK	[gemSpec_Kry pt], Kap. 6 (VAU)	Schlüssellänge entsprechend der	[gemSpec _Krypt], Kap. 6	FCS_COP.1.1/VAU.Auth

		und Verifikation für das VAU Protokoll ecdsa-with-Sha256 (OID 1.2.840.10045.4.3.2)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256)	verwendeten elliptischen Kurve brainpoolP256 r1 ([RFC5639])		
15.	Schlüsse-laushand-lung	Diffie-Hellman Schlüsselaushandlung (DH) für VPN (IPsec IKEv2, diffie-hellman group 14)	[HaC] (DH) [RFC-3526] (DH Group) [RFC-7296] (IKEv2) Siehe Abwei-chungen: [14], Kap. 4	DH: Gruppe 14 2048 Bit Exponentenläng ge 2047 Bits	[gemSpec _Krypt], Kap. 3.3.1	FCS_CKM.2/NK.IKE
16.		Elliptic Curve Diffie-Hellman Schlüssel-aushandlung (ECDH) für VPN	[SEC1] (ECDH), [RFC-7296] (IKEv2) [RFC-6954] (ECC curves for IKEv2)	Schlüssel-länge entspre-chend der ver-wendeten el-liptischen Kur-ven brain-poolP256r1 ([RFC-6954])	[gemSpec _Krypt], Kap. 3.3.1 und Kap. 5.5	FCS_CKM.2/NK.IKE
17.		Diffie-Hellman Schlüsselaushandlung (DH) und Elliptic Curve Diffie-Hellman Schlüsselaushandlung (ECDH) für TLS	[HaC] (DH) [SEC1] (ECDH), [RFC-5246] (TLS v1.2) [RFC-3268] (DHE_RSA) [RFC-4492] (ECDHE_RSA) [RFC-3526] (DH Gruppe 14) Siehe Abwei-chungen: [14], Kap. 4	DH: Gruppe 14 2048 Bit Exponentenläng ge = 2048 Bits ECDH: Schlüssellänge entsprechend der verwendeten elliptischen Kurven P-{256,384} ([FIPS186-4]) und brainpoolP{256, 384}r1 ([RFC7027])	[gemSpec _Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS
18.		Elliptic Curve Diffie-Hellman Schlüsselaushandlung (ECDH) für VAU Protokoll	[gemSpec_Kry pt], Kap. 6 (VAU) [NIST-800-56-A#5.7.1.2] (ECDH) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpoolP256 r1 ([RFC5639])	[gemSpec _Krypt], Kap. 6	FCS_CKM.1/VAU
19.	Schlüsse-	HMAC Berechnung	[IANA] mit [RFC-8247],	128 Bit und	[gemSpec _Krypt],	FCS_COP.1/NK.HMAC

	lableitung	für VPN (PRF) PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	#2.2 [FIPS 180-4] (SHA) [RFC-2404] (HMAC) [RFC-7296] (IKEv2)	256 Bit	Kap. 3.3.1	
20.		Schlüsselableitung für TLS 1.2	[RFC-5246] (TLS v1.2) [FIPS-180-4] (SHA) [RFC-2104] (HMAC)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS
21.		Schlüsselableitung mit HKDF für das VAU Protokoll	[gemSpec_Krypt], Kap. 6 (VAU) [FIPS 180-4] (SHA) [RFC-5869] (HKDF)	256 Bit	[gemSpec_Krypt], Kap. 6 (VAU)	FCS_CKM.1/VAU
22.	Schlüssel-generierung	RSA Schlüssel generierung im X.509 und PKCS#12 Format	[RFC4055] (sup. [RFC5280]), [RFC7292] (PKCS#12) [FIPS186-4] (Method B.3.3) Siehe Abweichungen: [14], Kap. 4	2048 Bit	TR 03116-1	FCS_CKM.1/NK.Zert
23.		ECC Schlüssel generierung im X.509 Format Elliptic Kurve Key Pair Generation	[TR-3111] (ECKeyPair) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639])	TR 03116-1	FCS_CKM.1/NK.Zert
24.	Integrität	HMAC Berechnung und Prüfung für VPN HMAC mit SHA-1, SHA-256	[FIPS 180-4] (SHA) [RFC-2104] (HMAC) [RFC-2404] (HMAC-SHA-1 mit ESP) [RFC-4868] (HMAC-SHA-2 mit IPsec) [RFC-7296] (IKEv2)	160 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.HMAC
25.		HMAC Berechnung und Prüfung für TLS	[FIPS 180-4] (SHA) [RFC-2104]	160 Bit, 256 Bit und 384 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/ NK.TLS.HMAC

		HMAC mit SHA-1, SHA-256 und SHA-384	(HMAC) [RFC-5246] (TLS v1.2)			
26.	Vertraulichkeit	Symmetrische Verschlüsselung und Entschlüsselung bei IKE und ESP für VPN Kommunikation AES-CBC (OID 2.16.840.1.101.3.4.1.42)	[FIPS 197] (AES) [RFC-3602] (AES-CBC) [RFC-4303] (ESP) [RFC-4301] (IPsec)	256 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
27.		Symmetrische Verschlüsselung und Entschlüsselung für TLS v1.2 AES-128 und AES-256 in CBC	[FIPS 197] (AES) [RFC-3602] (AES-CBC) [RFC-3268] (AES-TLS mit DH) [RFC-4492] (AES-TLS mit ECDH)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/ NK.TLS.AES
28.	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	AES-128 und AES-256 in GCM Mode für TLS 1.2	[FIPS 197] (AES) [RFC-3268] (AES-TLS) [SP 800-38D] (GCM) [RFC-5289] (AES-GCM-TLS) [RFC-5116] (AEAD)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/ NK.TLS.AES
29.		Symmetrische Verschlüsselung und Entschlüsselung bei IKE und ESP für VPN Kommunikation AES-GCM-128 und AES-GCM-256 mit 12 und 16 Byte großem ICV	[FIPS 197] (AES) [RFC-4303] (ESP) [RFC-4301] (IPsec) [RFC-4106] (AES-GCM)	AES-GCM: 128 und 256 Bit und 128 Bit Tag Länge	[gemSpec_Krypt], Kap. 3.3.1 und Kap. 5.5	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
30.		AES-256 in GCM Mode für VAU Kommunikation	[gemSpec_Krypt], Kap. 6 (VAU) [FIPS 197] (AES) [SP 800-38D] (GCM) [RFC-5116] (AEAD)	256 Bit und 128 Bit Tag-Länge	[gemSpec_Krypt], Kap. 6	FCS_COP.1/VAU.AES
31.		ECIES basierte hybride Verschlüsselung und Entschlüsselung mit Nachrichtenauthentiz	[gemSpec_Krypt], Kap. 3.15 (SGD) [SEC1-2009]	ECDH: Schlüssellänge entspre-	[gemSpec_Krypt], Kap. 3.15	FCS_COP.1/ SGD.ECIES

		ität und ECC Schlüsselgenerierung mittels ECIES mit brainpoolP256r1, HKDF mit SHA-256 und AES-256 in GCM Mode	(ECIES) [NIST-800-56-A#5.7.1.2] (ECDH) [RFC-5639] (brainpool) [FIPS 180-4] (SHA) [RFC-5869] (HKDF) [FIPS 197] (AES) [SP 800-38D] (GCM) [RFC-5116] (AEAD)	chend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639]) AES-GCM: 256 Bit AES und 128 Bit Tag länge		
32.	Sichere Kanäle	TLS v1.2	[RFC-5246] (TLS v1.2) [SMD3_AK] [SMD3_MS_AK]	-	[gemSpec_Krypt], Kap. 3.3.2	FTP_ITC.1/NK.TLS FTP_TRP.1/NK.Admin
33.		VPN IPsec (IKEv2) mit Zertifikatbasierter Authentisierung	[RFC-4301] (IPsec) [RFC-4303] (ESP) [RFC-7296] (IKEv2) [SMD3_NK] [SMD3_MS]	-	[gemSpec_Krypt], Kap. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS
34.		VAU Protokoll Kommunikation entsprechend der Vorgaben des ePA-Aktensystems für den Austausch von Nachrichtenmit der VAU	[gemSpec_Krypt], Kap. 6 (VAU)	-	[gemSpec_Krypt], Kap. 6	FTP_ITC.1/VAU
35.		SGD Protokoll (ECIES) Kommunikation entsprechend der Vorgaben des ePA-Aktensystems für den Austausch von Nachrichten mit dem SGD-HSM	[gemSpec_Krypt], Kap. 3.15 (SGD)	-	[gemSpec_Krypt], Kap. 3.15	FTP_ITC.1/SGD Anmerkung: Die abgesicherte Kommunikation zwischen SGD-Klient und SGD-HSM wird als Sicherer Kanal (trusted channel) im ST [6] modelliert.
36.	Authentizität	PAdES basierte Signaturerzeugung mit SHA-256 und	[RFC-8017] (PKCS#1) [TR-03111] ECDSA [RFC-5639]	RSA: 1976 Bit bis 4096 Bit ECC:	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt],	Signatur Verifikation: FDP_DAU.2/AK.Sig FDP_DAU.2/AK.QES

		Unterstützungvon HBA oder SMC-B und Verifikation mit SHA-{256, 384, 512} im Format RSASSA-PKCS1-v1_5 RSASSA-PSS und ECDSA (nur für SHA-256)	brainpool [PAdES] [PAdES_BP] [FIPS 180-4] (SHA)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639])	Kap. 3.8	FCS_COP.1/ AK.SigVer.SSA FCS_COP.1/ AK.SigVer.PSS FCS_COP.1/ AK.SigVer.ECDSA FCS_COP.1/ AK.PDF.SigPr Hash: FCS_COP.1/AK.SHA Generierung des signierten Dokumentes: FCS_COP.1/ AK.PDF.Sign Die digitalen Signaturen werden durch die Chipkarten erzeugt.
37.		CAdES basierte Signaturerzeugung mit SHA-256 und Unterstützung von HBA oder SMC-B und Verifikation mit SHA-{256, 384, 512} im Format RSASSA-PKCS1-v1_5 RSASSA-PSS und ECDSA (nur für SHA-256)	[RFC-8017] (PKCS#1) [TR-03111] ECDSA [RFC-5639] brainpool RFC-5652] (CMS) [CAdES] [CADES_BP] [FIPS 180-4] (SHA)	RSA: 1976 Bit bis 4096 Bit ECC: Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 3.12 [gemSpec_Krypt], Kap. 3.7	Signatur Verifikation: FDP_DAU.2/AK.Sig FDP_DAU.2/AK.QES FCS_COP.1/ AK.SigVer.SSA FCS_COP.1/ AK.SigVer.PSS FCS_COP.1/ AK.SigVer.ECDSA FCS_COP.1/ AK.CMS.SigPr Hash: FCS_COP.1/AK.SHA Generierung des signierten Dokumentes: FCS_COP.1/ AK.CMS.Sign Die digitalen Signaturen werden durch die Chipkarten erzeugt.
38.		XAdES basierte Signaturerzeugung mit	[RFC-8017] (PKCS#1) [TR-03111] ECDSA	RSA: 1976 Bit bis 4096 Bit	[gemSpec_Krypt], Kap. 3.12	Signatur Verifikation: FDP_DAU.2/AK.QES

		SHA-256 und Unterstützung von HBA oder SMC-B und Verifikation mit SHA-{256, 384, 512} im Format RSASSA-PKCS1-v1_5 RSASSA-PSS und ECDSA (nur für SHA-256)	[RFC-5639] brainpool [XMLSig] [XAdES] [XAdES_BP] [FIPS 180-4] (SHA)	ECC: Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 3.1	FCS_COP.1/ AK.SigVer.SSA FCS_COP.1/ AK.SigVer.PSS FCS_COP.1/ AK.SigVer.ECDSA FCS_COP.1/ AK.XML.SigPr Hash: FCS_COP.1/AK.SHA Generierung des signierten Dokumentes: FCS_COP.1/ AK.XMLS.Sign Die digitalen Signaturen werden durch die Chipkarten erzeugt.
39.	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	Hybride Dokumenten Ver- und Entschlüsselung (XML, CMS) mit RSAES-OAEP und AES-GCM	[FIPS 197] (AES) [SP 800-38D] (AES GCM) [RFC-8017] (RSAOAEP) [XMLEnc] (XML) [RFC-5652] (CMS)	RSA ENC: 2048 Bit (RSAOAEP) AES-GCM-ENC: 256 Bit AES-GCM-DEC: 128, 192, 256 Bit	[gemSpec_Krypt], Kap. 3.1.5 und 3.5	FCS_COP.1/AK.AES FCS_COP.1/ AK.XML.Ver FCS_COP.1/ AK.XML.Ent FCS_COP.1/ AK.CMS.Ver FCS_COP.1/ AK.CMS.Ent Die Asymmetrische Entschlüsselung des AES Schlüssels wird durch die Chipkarten durchgeführt (HBA, SMC-B oder eGK)
40.		Hybride Dokumenten Ver- und Entschlüsselung (XML, CMS) mit ECIES und AES-GCM für Dokument Ver- und Entschlüsselung	[gemSpec_COS] Kapitel 6.8.1.4 (ECIES) [RFC-5639] (brainpool) [FIPS 197] (AES) [SP 800-38D] (AES GCM) [XMLEnc] (XML) [RFC-5652] (CMS) Siehe Abweichungen: [14], Kap. 4	ECC: Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainpool-P256r1 ([RFC5639]) AES-GCM-ENC: 256 Bit AES-GCM-DEC: 128, 192, 256 Bit	[gemSpec_Krypt], chap. 5.7	FCS_COP.1/AK.AES FCS_COP.1/ AK.XML.Ver FCS_COP.1/ AK.XML.Ent FCS_COP.1/ AK.CMS.Ver FCS_COP.1/ AK.CMS.Ent ECIES Entschlüsselung wird mit Unterstützung der Chipkarten durchgeführt (HBA, SMC-B oder eGK)

41.	Schlüsse-lerzeu-gung	AES Schlüsselerzeugung für Hybride Verschlüsselung durch Verwendung sicherer Zufallszahlen	[SP800-133], Kap. 6.1 (Schlüsselerze ugung)	256 Bit	[gemSpec _Krypt], Kap. 3.1.5 und 3.5	Erzeugung von AES Schlüsseln: FCS_CKM.1/AK.AES

Tabelle 3: kryptografische Funktionen des EVG

Gemäß [gemSpec_Krypt] und [TR03116-1] sind die Algorithmen geeignet für den jeweiligen Zweck.

Die folgende Tabelle gibt einen Überblick über die im EVG enthaltene Update-Funktionalität und legt deren Bewertung des Sicherheitsniveaus aus kryptographischer Sicht dar.

#	Zweck	Kryptographischer Mechanismus	Implementie-rungsstan-dard	Schlüssel-länge in Bit	Sicher-heitsniveau über 100 Bit	Kommentar
1.	Authentizität	GPG RSA Signatur Verifikation mit RSASSA-PKCS1-1.5 unter Anwendung von SHA-512	[RFC-4880] (OpenPGP) [RFC-8017] (RSA) [FIPS 180-4] (SHA)	2048 Bit	Ja	Signature Verifikation des Firmware Updates FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
2.		RSA Signatur Verifikation mit RSASSA-PSS unter Anwendung von SHA-256	[RFC-8017] (RSA), [FIPS 180-4] (SHA)	4096 Bit	Ja	Signatur Verifikation von UpdateInfo.xml und FirmwareGroupInfo.xml FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
3.	Schlüsseler-zeugung	Backup Encryption-Schlüsselerzeu-gung unter Anwendung eines sicheren Zufalls-zahlengenerators	AK-Sicherheits-architektur	256 Bit	Ja	FMT_MTD.1/ AK.eHKT_Abf
4.	Vertraulichkeit mit Nachrich-tenauthentizi-tät (Authentic-ated Encryp-tion)	Hybride Verschlüsselung von Backups mittels RSAOAEP und AES-GCM Password basierte Verschlüsselung des Backup Schlüssels mit AES-ECB	[RFC-8017] (RSAOAEP) [FIPS 197] (AES) [NIST-SP-800-38A] (AES ECB) [NIST-SP-800-38D] (AES GCM) [PKCS5] (PBE) AK-Sicherheits-architektur	RSA: 2048 Bit AES-GCM: 256 Bit Passwort: >120 Bit	Ja	FMT_MTD.1/ AK.eHKT_Abf

Tabelle 4: Kryptografische Funktionen des EVG (Update und Backup)

Die kryptografische Stärke dieser Algorithmen 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.

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:

Der EVG kann seine Sicherheitsleistung nur unter den folgenden Bedingungen erbringen:

- Die EVG-Konfiguration sieht eine verpflichtende Nutzung von TLS sowie eine verpflichtende Client-System-Authentisierung vor.
- Die angeschlossenen Client-Systeme verifizieren die Authentizität des Konnektors, wenn sie dessen Dienste nutzen oder Ereignisse empfangen.
- Der Benutzer ist in der Lage zu identifizieren, dass die Verbindung zu einem Client-System sicher ist.

Der EVG-Benutzer soll (shall) den EVG nur dann betreiben, wenn die oben genannten Bedingungen erfüllt sind. Ein Verstoß oder eine Nichterfüllung dieser Bedingungen wird als eine Schwachstelle des EVG bezüglich der Einsatzumgebung verstanden. In diesem Fall ist der EVG-Benutzer dafür verantwortlich Gegenmaßnahmen gegen diese Schwachstelle zu ergreifen.

Der EVG unterstützt unterschiedliche Betriebskonfigurationen. Die wesentlichen Konfigurationen sind: „Parallel”-, „inReihe”- und „Offline“-Modus. Die empfohlene Konfiguration ist der Konfigurationsmodus „inReihe”, da dieser eine höhere Sicherheit der

angeschlossenen LAN-seitigen Netzwerke bietet, siehe Bedienhandbuch [10] [a], Kapitel 10.2.1.2 Anbindungsmodus.

Für aktive VPN-Verbindungen, die IPSec nutzen, sind im EVG keine Gegenmaßnahmen gegen die statistische Datenverkehrsanalyse implementiert.

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

AK Anwendungskonnektor

AMTS Arzneimitteltherapiesicherheit

BIOS Basic Input/Output System

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

CRL Certificate Revocation List

CVC Card Verifiable Certificate

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DTBS Data To Be Signed

EAL Evaluation Assurance Level – Vertrauenswürdigkeitsstufe

eGK Elektronische Gesundheitskarte

ePA Elektronische Patientenakte

ESP Encapsulating Security Payload

ETR Evaluation Technical Report

EVG Evaluierungsgegenstand – Target of Evaluation (TOE)

GCM Galois/Counter Mode

gSMC-K	Sicherheitsmodul für den Konnektor
HBA	Heilberufsausweis
HMAC	Keyed-Hash Message Authentication Code
ICCSN	Integrated Circuit Card Serial Number
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
KSR	Konfigurations- und Software-Repository
LAN	Local Area Network
NFDM	Notfalldatenmanagement
NK	Netzkonnektor
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PP	Protection Profile – Schutzprofi
PTV	Produkttyp Version
QES	Qualifizierte Elektronische Signatur
SAR	Security Assurance Requirement – Vertrauenswürdigkeitsanforderungen
SGD	Schlüsselgenerierungsdienst
SHA	Secure Hash Algorithm
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
SICCT	Secure Interoperable Chip Card Terminal
SIS	Secure Internet Service
ST	Security Target – Sicherheitsvorgaben
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation – Evaluierungsgegenstand (EVG)
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
TSL	Trust-service Status List
VPN	Virtual Private Network
VAU	Vertrauenswürdige Ausführungsumgebung

VSDM Versichertenstammdatenmanagement

WAN Wide Area Network

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

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/zertifizierungsreporte

[6] Sicherheitsvorgaben BSI-DSZ-CC-1201-2022, Version 1.2, 27.06.2022, Security Target für secunet konnektor 2.0.0 (eHealth Konnektor PTV5 WR1), secunet Security Networks AG

[7] Evaluierungsbericht, Version 1.7, 10.08.2022, Evaluation Report - Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH (vertrauliches Dokument)

[8] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-01, Version 1.6, 30.03.2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] Dokument zur sicheren Lieferkette:

secunet(konnektor Version 2.0.0 und 2.1.0, Hinweise zur sicheren Lagerung und Lieferkette, Version 1.9, 04.11.2019

[10] EVG-Handbücher:

[a] secunet(konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Bedienungsanleitung, Für Administratoren und Benutzer, Version 6.1, 09.06.2022, secunet Security Networks AG. Inklusive Errata der Bedienungsanleitung Version 6.1 vom 09.06.2022, Version 1.0, 27.06.2022

[b] secunet(konnektor v2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 1.8, 31.10.2019

[c] Konnektor Management API-Dokumentation, Version 5.0.0, Stand 11.05.2022, eHealth Experts GmbH, Dateiname: konnektor-rest-doc-5.0.0-Konnektor-FW-5.1.1.pdf

[d] Security Guidance Fachmodulentwicklung, Version 1.5; 19.04.2021, eHealth Experts GmbH, Dateiname: Security Guidance Fachmodulentwicklung_v1.5.pdf

[11] Konfigurationsliste für den EVG (vertrauliche Dokumente)

220614_ALC_CMS_Modularer-Konnektor_NK-Implementierung_v3.2

1201_1044-V6_1202_1128-V5_References_secunet_konnektor v1.4.pdf

Konfigurationsliste (ALC_CMS.4), Version 8.1, Datei: ALC_CMS_eHX_v8.1.xls

[9] insbesondere

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- 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)

Konfigurationsliste (ALC_CMS), Regulatory Affairs Document, Rev# 4.00, 01.07.2020

[12] Referenzen von Implementierungsstandards:

[HaC] A. Menezes, P. van Oorschot und O. Vanstone. Handbook of Applied Cryptography. CRCPress, 1996.

[FIPS180-4] NIST: FIPS PUB 180-4 Secure Hash Signature Standard (SHS), March 2012

[FIPS186-4] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 186-4: Digital Signature Standard (DSS); National Institute of Standards and Technology, July 2013

[FIPS197] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[IANA] Internet Key Exchange Version 2 (IKEv2) Parameters, iana https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-6

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997

[RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH, Network Working Group, November 1998

[RFC3268] Chown, P., Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS), RFC 3268, June 2002

[RFC3526] T. Kivinen, M.Kojo: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). May 2003

[RFC3602] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003

[RFC4301] S. Kent, K. Seo: Security Architecture for the Internet Protocol, December 2005

[RFC4303] S. Kent: IP Encapsulating Security Payload (ESP), December 2005

[RFC4346] T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006

[RCF4492] Blake-Wilson, et al.: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), May 2006

[RFC4868] S. Kelly, S. Frankel: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, May 2007

[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer: OpenPGP Message Format, November 2007

[RFC5246] T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008

[RFC5289] E. Rescorla, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

[RFC5996] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen: Internet Key Exchange (IKEv2) Protocol, September 2010

[RFC7027] J. Merkle, M. Lochter, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), October 2013

[RFC7296] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014

[RFC8017] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch: PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016

[SMD3_AK] RFC-Analyse AK-TLS, Anwendungskonnektor, Version 1.1, 26. Oktober 2018

[SMD3_MS_AK] Nachweis TLS Security, Version 0.9, 26. April 2018, TLSv11_MAY+SHOULD_26.04_final.xlsx

[SMD3_NK] secunet(konnektor Version 2.0.0, VPN-Analyse, Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, Version 0.97, 16. August 2018

[SMD3_MS] IPsec-RFCs - MAY_SHOULD Anforderungen, secunet(konnektor, Version 0.95, 22.07.2018

[SP800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007

[RFC4106] The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), June 2005, https://www.rfc-editor.org/rfc/rfc4106.html

[GCM] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf, January 2004.

[13] Referenzen auf Anwendungsstandards:

[gemSpec_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec_Kon], PTV5: Version 5.15.0, 31.01.2022, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.21.0, 31.01.2022

[gemSpec_Net] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 1.21.0, 21.01.2022

[TR03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20, 21.09.2018, Technische Arbeitsgruppe TR-03116

[TR-03154] Konnektor – Prüfspezifikation für das Fachmodul NFDM, Technische Richtlinie BSI TR-03154, Version 1.1, 15.04.2019

[TR-03155] Konnektor – Prüfspezifikation für das Fachmodul AMTS, Technische Richtlinie BSI TR-03155, Version 1.1, 15.04.2019

[TR-03157] BSI TR-03157 Konnektor – Prüfspezifikation für das Fachmodul ePA, Technische Richtlinie BSI TR-03157, Version 2.0, 03.08.2021

[14] Cryptographic conformity assessment - Kryptographische Mechanismen des secunet eHealth konnektor 2.0.0 und 2.1.0 (PTV5 WR1), Version 0.8, 10.08.2022, Dateiname: 1184_AVA_CCA_20220810_v08, SRC Security Research & Consulting GmbH (vertrauliches Dokument)

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