

**BSI-DSZ-CC-1135-2020**

ZU

**secunet konnektor 2.0.0, Version 3.5.0:2.0.0**

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-1135-2020 (\*)

Gesundheitswesen: Konnektoren

**secunet konnektor 2.0.0**, Version 3.5.0:2.0.0

von **secunet Security Networks AG**  
PP-Konformität: **Common Criteria Schutzprofil (Protection Profile)  
Schutzprofil 2: Anforderungen an den Konnektor,  
Version 1.5.4, BSI-CC-PP-0098-V2-2020 vom  
17.03.2020**  
Funktionalität: **Produktspezifische Sicherheitsvorgaben  
Common Criteria Teil 2 erweitert**  
Vertrauenswürdigkeit: **Common Criteria Teil 3 konform  
EAL 3 mit Zusatz von ADV\_FSP.4, ADV\_TDS.3,  
ADV\_IMP.1, ALC\_TAT.1, AVA\_VAN.3 und  
ALC\_FLR.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.

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, 6. November 2020

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Sandro Amendola  
Abteilungspräsident

L.S.



Common Criteria  
Recognition Arrangement  
Anerkennung nur für  
Komponenten bis EAL 2  
und ALC\_FLR



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

1. Vorbemerkung.....	6
2. Grundlagen des Zertifizierungsverfahrens.....	6
3. Anerkennungsvereinbarungen.....	7
4. Durchführung der Evaluierung und Zertifizierung.....	8
5. Gültigkeit des Zertifizierungsergebnisses.....	8
6. Veröffentlichung.....	9
B. Zertifizierungsbericht.....	10
1. Zusammenfassung.....	11
2. Identifikation des EVG.....	17
3. Sicherheitspolitik.....	19
4. Annahmen und Klärung des Einsatzbereiches.....	19
5. Informationen zur Architektur.....	20
6. Dokumentation.....	21
7. Testverfahren.....	21
8. Evaluerte Konfiguration.....	24
9. Ergebnis der Evaluierung.....	24
10. Auflagen und Hinweise zur Benutzung des EVG.....	31
11. Sicherheitsvorgaben.....	32
12. Definitionen.....	32
13. Literaturangaben.....	35
C. Auszüge aus den Kriterien.....	39
D. Anhänge.....	40

## 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<sup>1</sup>
- BSI-Zertifizierungs- und -Anerkennungsverordnung<sup>2</sup>
- BSI-Kostenverordnung<sup>3</sup>
- 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<sup>4</sup> [1], auch als Norm ISO/IEC 15408 veröffentlicht.

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

<sup>2</sup> 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

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

<sup>4</sup> Bekanntmachung des Bundesministeriums des Innern vom 12. Februar 2007 im Bundesanzeiger, datiert 23. Februar 2007, S. 1941

- 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. Anerkennungvereinbarungen

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.

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+ 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 3.5.0:2.0.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts secunet konnektor 2.0.0, Version 3.5.0:2.0.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 14. August 2020 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)<sup>5</sup>

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 Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierungs- 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.

<sup>5</sup> Information Technology Security Evaluation Facility

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 6. November 2020, ist gültig bis 5. November 2025. 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 Weitergaberegulung 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 3.5.0:2.0.0 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<sup>6</sup>. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

<sup>6</sup> secunet Security Networks AG  
Kurfürstenstraße 58  
45138 Essen

## **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, bestehend aus dem Netzkonnektor und dem Anwendungskonnektor nach dem Protection Profile [9].

Der Netzkonnektor umfasst die Sicherheitsfunktionen einer Firewall und eines VPN-Clients sowie einen NTP-Server, einen Namensdienst (DNS) und einen DHCP-Dienst. 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.

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\_TDS.3, ADV\_IMP.1, 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 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
<b>Sicherheitsfunktionalität des NK als Teil des EVG</b>	
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 vorgelegt und können vom Administrator für den SIS verwaltet werden.

Sicherheitsfunktionalität des EVG	Thema
Netzdienste: Zeitsynchronisation	<p>Der EVG führt bei bestehender Verbindung zur TI in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch.</p> <p>Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand am Gehäuse des Konnektors anzeigt.</p>
Netzdienste: Zertifikatsprüfung	<p>Der EVG überprüft die Gültigkeit der Zertifikate, die für den Aufbau der VPN-Kanäle 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.</p>
Stateful Inspection	<p>Packet</p> <p>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.</p>
Selbstschutz: Speicheraufbereitung	<p>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.</p>
Selbstschutz: Selbsttests	<p>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 (Secure Boot) kann nicht deaktiviert bzw. manipuliert werden.</p> <p>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.</p>
Selbstschutz: Schutz von Geheimnissen, Seitenkanalresistenz	<p>Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme. Dies gilt grundsätzlich für kryptographisches Schlüsselmaterial.</p> <p>Der private Authentisierungsschlüssel für das VPN wird bereits durch die gSMC-K und dessen 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.</p>
Selbstschutz: Sicherheits-Log	<p>Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation.</p>
Administration	<p>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.</p> <p>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.</p> <p>Die Administration der Filterregeln für den dynamischen Paketfilter ist den Administratoren vorbehalten.</p>

Sicherheitsfunktionalität des EVG	Thema
Software Update	<p>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.</p> <p>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-Paketes analog zum regulären Boot-Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können.</p>
Kryptographische Basisdienste	<p>Der Konnektor implementiert Kryptographische Basisdienste für den Aufbau von sicheren VPN-Verbindungen zu den VPN-Konzentratoren der TI und des SIS.</p>
<p>TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen</p>	<p>Der Netzkonnektor stellt dem Anwendungskonnektor die Dienste zum Aufbau eines TLS-Kanals zur Verfügung. TLS wird auch zur Absicherung der Administratorschnittstelle verwendet.</p> <p>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).</p> <p>Zertifikate die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen, werden vom Netzkonnektor entsprechend den Anforderungen in [gemSpec_Kon] interpretiert. Der EVG prüft insbesondere, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist enthalten ist.</p> <p>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 Clientsysteme können auch vom EVG über die gesicherte Management-Schnittstelle durch den Administrator importiert werden, um ggfls. benötigte Betriebszustände wiederherzustellen.</p> <p>Die TLS-Verbindungen werden vom Anwendungskonnektor gemanagt und je nach Anwendungsfall eingerichtet.</p>
<b>Sicherheitsfunktionalität des AK als Teil des EVG</b>	
<p>Identifikation und Authentisierung</p>	<p>Der Konnektor setzt unterschiedliche Mechanismen zur Identifikation und Authentisierung von Benutzern um.</p> <p>Die Management-Schnittstelle des Konnektors ist durch Passwordeingabe vor unautorisiertem Zugriff geschützt. Dabei gelten die folgenden Anforderungen nach [13] [gemSpec_Kon], TIP1-A_4808 an die Administrator Passwörter.</p> <p>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.</p>
<p>Zugriffsberechtigungs-dienst</p>	<p>Der Zugriffsberechtigungs-dienst (oder Zugriffskontrolldienst) ist ein interner Dienst des Konnektors der automatisch bei Aufruf einer Operation des Konnektors durch</p>

Sicherheitsfunktionalität des EVG	Thema
	<p>das Clientsystem umgesetzt wird. Durch den Zugriffskontrolldienst wird eine Prüfung auf Zugriffsberechtigung für die an-geforderten Ressourcen durchgeführt.</p> <p>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.</p>
Kartenterminaldienst	<p>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.</p> <p>Der Anwendungskonnektor kommuniziert mit den konfigurierten eHealth-Kartenterminals über TLS-Kanäle. Der Netzkonnektor stellt diese Kommunikationskanäle kontrolliert dem Anwendungskonnektor zur Verfügung.</p> <p>Informationen über die Arbeitsplatzkonfiguration eines angeschlossenen Kartenterminals können vom Kartenterminaldienst ausgegeben werden. Nur der Administrator darf diese Daten auch verändern.</p>
Kartendienst	<p>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. [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 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.</p>
Signaturdienst	<p>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 Signaturreichtlinie behandelt werden.</p> <p>Der Signaturdienst unterstützt nicht-qualifizierte elektronische Signaturen (nonQES) sowie qualifizierte elektronische Signaturen (QES), die mit Hilfe der vom Chipkartendienst verwalteten Chipkarten erzeugt werden.</p> <p>Der Signaturdienst unterstützt die folgenden Signaturformate für nonQES und QES:</p> <ul style="list-style-type: none"> <li>• XAdES für XML Dokumente (Nur QES mit NFDM-Signaturreichtlinie),</li> <li>• CAdES für XML, PDF/A, Text und TIFF Dokumente</li> <li>• PAdES für PDF/A Dokumente.</li> </ul> <p>Darüber hinaus werden für nonQES die folgenden Signaturformate unterstützt:</p> <ul style="list-style-type: none"> <li>• CAdES für Binärdokumente</li> </ul>

Sicherheitsfunktionalität des EVG	Thema
	<ul style="list-style-type: none"> <li>• S/MIME für Multipurpose Internet Mail Extensions,</li> </ul> <p>Zudem wird für nonQES und QES PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 unterstützt.</p> <p>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.</p>
Software-Update	<p>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 von Anwendungskonnektor und Netzkonnektor nur Update-Pakete erfolgreich installiert werden, deren Signatur erfolgreich geprüft wurde. Die Firmwaregruppe des Updates muss gleich oder höher der gegenwärtig installierten Firmwaregruppe sein.</p> <p>Der Updateprozess verhindert, dass manipulierte Update-Pakete eingespielt werden..</p> <p>Fachmodule können nur im Rahmen von Software-Updates des Konnektors aktualisiert oder eingebracht werden.</p>
Verschlüsselungsdienst	<p>Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an.</p> <p>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 und für MIME-Dokumente die hybride Ver-/Entschlüsselung nach [12] [S/MIME] unterstützt.</p> <p>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 Verschlüsselungszertifikate geprüft.</p>
TLS-Kanäle	<p>Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung. Die Verwaltung von TLS-Kanälen wird durch den Anwendungskonnektor durchgeführt.</p> <p>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.</p> <p>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).</p> <p>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.</p>

Sicherheitsfunktionalität des EVG	Thema
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	<p>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-Signaturreichtlinie geprüft.</p> <p>Der Konnektor setzt die in [13] [gemSpec_Kon], TAB_KON_503, definierten Fehlbetriebszustände um (Error Condition). Wird ein sicherheitsrelevanter Betriebszustand erreicht, schränkt der Konnektor seine Funktionalität gemäß [13] [gemSpec_Kon], TAB_KON_504, ein.</p> <p>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,</p> <p>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 (VPN 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.</p> <p>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</p>

Sicherheitsfunktionalität des EVG	Thema
	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.

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 3.2, 3.3 und 3.4 dar.

Dieses Zertifikat umfasst die in Kapitel 8 beschriebene Konfigurationen 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 3.5.0:2.0.0**

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifizier	Version	Auslieferungsart
1.	HW	secunet konnektor 2.0.0 Hardware für EBK (nicht Teil des EVG)	Hardware Version: 2.0.0 BIOS FW Version: CSASR007, CSASR009, CSASR011	Das Gerät wird über eine sichere Lieferkette dem Endkunden zugestellt.
2.	HW	gSMC-Ks (nicht Teil des EVG)	STARCOS 3.6 Health SMCK R1 (BSI-K-TR-0253-2016) oder TCOS Security Module Card - K Version 2.0 Release 1 (BSI-K-TR-0226-2015)	Die gSMC-Ks sind in der Konnektor-Hardware verbaut.



Nr	Typ	Identifizier	Version	Auslieferungsart
			Security Guidance Fachmodulentwicklung; eHealthExperts; v.1.3; 10.06.2020  SHA256: 19443C9A953A21C9D715C9EC0344A 53C826D800C05A19F61AFA2ED037F 005F3A	Die Security Guidance Fachmodulentwicklung wird nur intern den Fachmodul-Entwicklern zur Verfügung gestellt.

Tabelle 2: Auslieferungsumfang des EVG

Die sichere Lieferkette wird in den folgenden Dokumenten [9] und [10] [b] beschrieben.

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

Das Gerät, das den EVG beinhaltet, ist in einem Gehäuse untergebracht, und verfügt über die Hardwareanschlüsse, die für den Betrieb des Konnektors nötig 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, ob im secunet konnektor 2.0.0 bzw. secunet konnektor 2.1.0 gSMC-Ks vom Typ STARCOS (Wert 0) oder TCOS (Wert 1) verbaut sind (siehe [10] [a], Tabelle 18 bzw. [10] [a], Tabelle 20).

### 3. Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionalität des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte: 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. Daher setzt der EVG um, dass Sicherheitsfehlfunktionen unterbleiben und schützenswerte Daten nicht abfließen. Weitere Details hierzu können dem Security Target, [6], Abschnitt 6, entnommen werden.

### 4. Annahmen und Klärung des Einsatzbereiches

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

- OE.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 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
- Informationsflusskontrolle
- 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
- 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

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

- Konnektor-Basissystem
- Subsystem VPN
- TLS-Basis Subsystem
- Konnektormanagement Subsystem
- Laufzeitumgebung Subsystem
- Fachmodul-VSDM Subsystem
- Subsystem Anwendungskonnektor PTV3

## 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.

Bei Tests und Schwachstellenanalyse wurde systematisch das Angreiferpotential "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.

In den Fällen, bei denen die Tests nicht an der finalen Version, sondern an fwVersion 3.4.0 durchgeführt wurden, haben die Evaluatoren eine Analyse der Änderungen des EVG zwischen getesteter und finaler Version anhand der bereitgestellten Beschreibungen des Herstellers und insbesondere des Source-Codes durchgeführt. Die Evaluatoren kamen dabei zu dem Schluss, dass eine Wiederholung der Tests an der aktuellen EVG-Version nicht notwendig ist, da die jeweils getestete Sicherheitsfunktion sich nicht geändert hat und durch die anderen Änderungen am EVG nicht beeinflusst wird. Die an EVG-Version 3.4.0 erhaltenen Testergebnisse sind vollständig auf die finale EVG-Version 3.5.0 übertragbar.

### **Herstellertests**

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

Die Sicherheitsvorgaben [6] beschreiben nur eine einzelne Konfiguration für den EVG. In [6], Abschnitt 1.3.2 wird die sogenannte "Einbox-Lösung" als einzige Konfiguration des Evaluierungsgegenstandes angegeben.

#### Testumgebung ANKE

Für jeden Test existiert eine XML Datei, in der die notwendigen Informationen enthalten sind, um den Testfall auszuführen; unter anderem die von der Testumgebung auszuführenden Test-Module, deren Parameter und die Test-Evaluatoren.

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 Netzwerkfunktionen 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.

Die AK-Funktionalität wurde hauptsächlich mit der Test-Engine ConCuTE (ANKE) getestet. Der NK-Teil wurde mit der Test-Engine cons10t (ANKE) und in der Testumgebung NWTU geprüft.

### 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.

Weiterhin wurden alle automatisierten Testfälle der Herstellertestumgebung wiederholt.

### Testergebnisse

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen festgestellt.

### **Penetrationstests der Prüfstelle**

Alle Konfigurationen des EVG, die von dieser Evaluierung abgedeckt sind, wurden getestet.

### Testergebnisse

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen festgestellt. Es war kein Angriffsszenario, welches einen Angreifer mit hohem Angriffspotential (Enhanced-Basic) voraussetzt, in der Betriebsumgebung, wie sie im Schutzziel [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 die Konfiguration „Einbox-Lösung“ als einzige Konfiguration des EVG (siehe [6], Kapitel 1.3). Hierbei sind der Netzkonnektor und der Anwendungskonnektor in einer Box integriert und die gSMC-K ist sicher mit dem Gesamtkonnektor verbunden ist, so dass kein weiterer Schutz der Verbindung zwischen Gesamtkonnektor und gSMC-K erforderlich ist.

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 verwendet.

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

Die Verfeinerungen der Anforderungen an die Vertrauenswürdigkeit, wie sie in den Sicherheitsvorgaben beschrieben sind, wurden im Verlauf der Evaluation beachtet.

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\_TDS.3, ADV\_IMP.1, ALC\_TAT.1, AVA\_VAN.3 und ALC\_FLR.2

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.4, BSI-CC-PP-0098-V2-2020 vom 17.03.2020 [8]
- Funktionalität: Produktspezifische Sicherheitsvorgaben  
Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform  
EAL 3 mit Zusatz von ADV\_FSP.4, ADV\_TDS.3, ADV\_IMP.1,  
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	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Kryptographische Funktionalität des Netzkonnektors:					
Authentizität	RSA Signaturverifikation für VPN und TLS  sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC8017] (PKCS#1)  [FIPS180-4] (SHA)	2048	[gemSpec _Krypt] Kp. 3.3.1 und 3.3.2	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert
	Verifikation von Signaturen der TSL und CRL mit RSASSA-PSS  sha256WithRSAEncryption	[RFC-8017] (PKCS#1)  [FIPS 180-4] (SHA)  [RFC-6931] (XMLDSig)	2048	gemSpec _Krypt], chap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert
Authentisierung	RSA Signatur- generierung mit Unter- stützung der gSMC-K und -verifikation für VPN und TLS  sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC8017] (RSASSA- PKCS1-v1_5)  [FIPS180-4] (SHA)	2048	[gemSpec _Krypt] Kp. 3.3.1	FCS_COP.1/NK.Auth FCS_COP.1/NK.TLS.Auth
Schlüsselaushandlung	Diffie-Hellman Schlüsselaushandlung (DH) für VPN (IPsec IKEv2, diffie-hellman group 14)	[HaC] (DH)  [RFC3526] (DH Group)  [RFC7296] (IKEv2)	DH:  group 14, 2048 Bit  Exponent- Länge ≥ 384 Bit	[gemSpec _Krypt], Kp. 3.3.1	FCS_CKM.2/NK.IKE

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
	Diffie-Hellman (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] (EC-DHE_RSA) [RFC-3526] (DH Group 14)	DH: group 14, 2048 Bit, Exponentlänge = 2048 Bit  ECDH: Schlüsselgröße entspricht der verwendeten elliptischen Kurve P-{256,384} [FIPS 186-4] und brainpoolP{256, 384}r1 [RFC 7027]	[gemSpec_Krypt], Kp. 3.3.2	FCS_CKM.1/NK.TLS
Schlüsselableitung	HMAC Berechnung für VPN (PRF)  PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	[FIPS 180-4] (SHA) [RFC-2404] (HMAC) [RFC7296] (IKEv2)	128, 256	[gemSpec_Krypt], Kp. 3.3.1	FCS_COP.1/NK.HMAC
	KDF für TLS v1.2	[RFC-5246] (TLS v1.2) [FIPS-180-4] (SHA) [RFC-1321] (MD5) [RFC-2104] (HMAC)	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_CKM.1/NK.TLS
Schlüsselerzeugung	RSA Key Pair Generation in X.509 and PKCS#12 format	[RFC4055] (sup. [RFC5280]) [RFC7292] (PKCS#12) [FIPS186-4] (Method B.3.3)	2048	TR 03116-1	FCS_CKM.1/NK.Zert

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Integrität	HMAC Berechnung und Verifikation für VPN  HMAC mit SHA-1, SHA-256	[FIPS180-4] (SHA)  [RFC-2104] (HMAC)  [RFC-2404] (HMAC-SHA-1 für ESP)  [RFC-4868] (HMAC-SHA-2 für IPsec)  [RFC-7296] (IKEv2)	160, 256	[gemSpec_Krypt], Kp. 3.3.1	FCS_COP.1/NK.HMAC
	HMAC Berechnung und Verifikation für TLS  HMAC mit SHA-{1, 256, 384}	[FIPS180-4] (SHA)  [RFC-2104] (HMAC)  [RFC-5246] (TLSv1.2)	160, 256, 384	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.HMAC
Vertraulichkeit	Symmetrische Ver- und Entschlüsselung mit ESP und für VPN  AES-CBC (OID 2.16.840.1.101.3.4.1.42)	[FIPS 197] (AES)  [RFC-3602] (AES-CBC)  [RFC-4303] (ESP, IPsec)	256	[gemSpec_Krypt], Kp. 3.3.1	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
	Symmetrische Ver- und Entschlüsselung für TLS v1.2  AES-{128, 256} in CBC	[FIPS 197] (AES)  [RFC-3602] (AES-CBC)  [RFC-3268] (AES-TLS mit DH)  [RFC-4492] (AES-TLS mit ECDH)	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.AES

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Verschlüsselung mit Authentizität	AES-{128, 256} in GCM für TLS v1.2	[FIPS 197] (AES) [RFC-3268] (AES-TLS) [SP 800-38D] (GCM) [RFC-5289] (AES-GCM-TLS) [RFC-5116] (AEAD)	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.AES
Gesicherter Kanal	TLS v1.2	[RFC-5246] (TLS v1.2) [SMD3_AK] [SMD3_MS_AK]	-	[gemSpec_Krypt], Kp. 3.3.2	FTP_ITC.1/NK.TLS FTP_TRP.1/NK.Admin
	VPN (IKEv2/Ipsec) mit zertifikatsbasierter Authentisierung	[RFC-4301] (IPsec) [RFC-4303] (ESP) [RFC-7296] (IKEv2) [SMD3_NK] [SMD3_MS]	-	[gemSpec_Krypt], Kp. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS
Kryptographische Funktionalität des Anwendungskonnektors:					
Authentizität	PADES basierte Signaturerzeugung mit SHA-256 und Unterstützung von HBA, SMC-B und Verifikation mit RSASSA-PKCS1-v1_5 mit SHA-{256, 384, 512} und RSASSA-PSS mit SHA-{256, 384, 512} für QES und nonQES	[RFC-8017] (PKCS#1) [PadES] [PadES_BP] [FIPS 180-4] (SHA)	1976 - 4096	[gemSpec_Krypt], Kp. 3.12 und Kp. 3.8	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.PDF.SigPr Hash: FCS_COP.1/AK.SHA Generierung von signierten Dokumenten: FCS_COP.1/AK.PDF.Sign Die digitalen Signaturen werden von den Signatur-Smartcards erzeugt.

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
	<p>CAdES basierte Signaturerzeugung mit SHA-256 und</p> <p>Unterstützung von HBA, SMC-B und</p> <p>Verifikation mit RSASSA-PKCS1-v1_5 mit SHA-{256, 384, 512} und</p> <p>RSASSA-PSS mit SHA-{256, 384, 512} für QES und nonQES</p>	<p>[RFC-8017] (PKCS#1)</p> <p>RFC-5652] (CMS)</p> <p>[CAdES]</p> <p>[CADES_BP]</p> <p>[FIPS 180-4] (SHA)</p>	1976 - 4096	[gemSpec_Krypt], Kp. 3.12 und Kp. 3.7	<p>Signatur-Verifikation:</p> <p>FDP_DAU.2/AK.Sig</p> <p>FCS_COP.1/AK.SigVer.SSA</p> <p>FCS_COP.1/AK.SigVer.PSS</p> <p>FCS_COP.1/AK.PDF.SigPr</p> <p>Hash:</p> <p>FCS_COP.1/AK.SHA</p> <p>Generierung von signierten Dokumenten:</p> <p>FCS_COP.1/AK.CMS.Sign</p> <p>Die digitalen Signaturen werden von den Signatur-Smartcards erzeugt.</p>
	<p>XAdES basierte Signaturerzeugung mit SHA-256 und</p> <p>Unterstützung von HBA, SMC-B und</p> <p>Verifikation mit RSASSA-PKCS1-v1_5 mit SHA-{256, 384, 512} und</p> <p>RSASSA-PSS mit SHA-{256, 384, 512} für QES und nonQES</p>	<p>[RFC-8017] (PKCS#1)</p> <p>[XMLSig]</p> <p>[XAdES]</p> <p>[XadES_BP]</p> <p>[FIPS 180-4] (SHA 256)</p>	1976 - 4096	[gemSpec_Krypt], Kp. 3.12 und Kp. 3.1	<p>Signatur-Verifikation:</p> <p>FDP_DAU.2/AK.Sig</p> <p>FCS_COP.1/AK.SigVer.SSA</p> <p>FCS_COP.1/AK.SigVer.PSS</p> <p>FCS_COP.1/AK.XML.SigPr</p> <p>Hash:</p> <p>FCS_COP.1/AK.SHA</p> <p>Generierung von signierten Dokumenten:</p> <p>FCS_COP.1/AK.XML.Sign</p> <p>Die digitalen Signaturen werden von den Signatur-Smartcards erzeugt.</p>
	<p>Verifikation von signierten Binärdaten mit</p> <p>RSASSA-PKCS1-v1_5 mit SHA-256 und</p> <p>RSASSA-PSS mit SHA256</p>	<p>[RFC-8017] (PKCS#1)</p> <p>[FIPS 180-4] (SHA)</p>	1976 - 4096	[gemSpec_Krypt], Kp. 3.12	<p>FDP_DAU.2/AK.Sig</p> <p>FCS_COP.1/AK.PKCS.SigPr</p> <p>FCS_COP.1/AK.SHA</p>

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Verschlüsselung mit Authentizität	Hybride Dokumenten (XML, MIME, CMS) Ver- und Entschlüsselung mit RSAES-OAEP und AES-GCM	[FIPS 197] (AES) [SP 800-38D] (AES GCM) [RFC-8017] (RSAOAEP) [XMLEnc] (XML) [RFC-5751] (S/MIME) mit [RFC-5083] (CMS Authenticated-Enveloped-Data Content Type) [RFC-5084] (AES-GCM in CMS) [RFC-5652] (CMS)	RSA-ENC: 2048 RSA-DEC: abhängig von der Karte AES-GCM-ENC: 256 AES-GCM-DEC: 128, 192, 256	[gemSpec_Krypt], Kap. 3.1.4 und 3.6 [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.MIME.Ver FCS_COP.1/AK.CMS.Ver FCS_COP.1/AK.MIME.Ent FCS_COP.1/AK.CMS.Ent  Asymmetrische Entschlüsselung des AES-Schlüssels erfolgt mittels einer Chipkarte (HBA, SMC-B oder eGK)
Schlüsselgenerierung	AES-Schlüsselgenerierung für hybride Verschlüsselung durch Verwendung eines sicheren Zufallszahlengenerators	[SP800-133, Kp. 7.1] (Key-Gen)	256	[gemSpec_Krypt], Kap. 3.1.5 und 3.5	Generierung des AES-Schlüssels: 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 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 Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>) entnommen werden.

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

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Sicherheitsniveau mehr als 100 Bit	Bemerkungen
Kryptographische Funktionalität des Netzkonnektors:					
Authentizität	GPG RSA Signaturverifikation mit Encoding RSASSA-PKCS1-1.5 und SHA-512	[RFC-4880] (OpenPGP) [RFC-8017] (RSA) [FIPS 180-4] (SHA)	2048	Ja	Signaturverifikation des Firmware Update FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
	RSA Signaturverifikation mit Encoding RSASSA-PSS und SHA-256	[RFC-8017] (RSA) [FIPS 180-4] (SHA)	4096	Ja	Signaturverifikation von UpdateInfo.xml und FirmwareGroupInfo.xml FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
Kryptographische Funktionalität des Anwendungskonnektors:					
Schlüsselgenerierung	Generierung des Backup-Verschlüsselungsschlüssels durch Verwendung eines sicheren Zufallszahlengenerators	[ARC_AK], s. [14]	256	Ja	FMT_MTD.1/AK.eHKT_Abf
Authenticated Encryption	Hybride Verschlüsselung des BackUps mit RSAOAE und AES-GCM Passwortbasierte Verschlüsselung des Backup-Schlüssels mit AES-ECB	[RFC-8017] (RSAOAE) [FIPS 197] (AES) [NIST-SP-800-38A] (AES ECB) [NIST-SP-800-38D] (AES GCM) [PKCS5] (PBE) [ARC_AK], s. [14]	RSA: 2048 AES-GCM: 256 Passwort > 120 Bit	Ja	FMT_MTD.1/AK.eHKT_Abf

Tabelle 4: Kryptografische Funktionen des EVG (Update-Mechanismus)

## 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

**AIS** Anwendungshinweise und Interpretationen zum Schema

<b>AMTS</b>	Arzneimitteltherapiesicherheit
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik
<b>cPP</b>	Collaborative Protection Profile
<b>EAL</b>	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
<b>eGK</b>	Elektronische Gesundheitskarte
<b>ESP</b>	Encapsulating Security Payload
<b>ETR</b>	Evaluation Technical Report
<b>EVG</b>	Evaluierungsgegenstand – Target of Evaluation (TOE)
<b>gSMC-K</b>	Sicherheitsmodul für den Konnektor
<b>HBA</b>	Heilberufsausweis
<b>HMAC</b>	Keyed-Hash Message Authentication Code
<b>IKE</b>	Internet Key Exchange Protocol
<b>IP</b>	Internet Protocol
<b>IPSec</b>	Internet Protocol Security
<b>IT</b>	Information Technology - Informationstechnologie
<b>ITSEF</b>	Information Technology Security Evaluation Facility - Prüfstelle für IT-Sicherheit
<b>KSR</b>	Konfigurations- und Software-Repository
<b>LAN</b>	Local Area Network
<b>MD5</b>	Message-Digest Algorithm 5
<b>NFDM</b>	Notfalldatenmanagement
<b>NK</b>	Network connector
<b>nonQES</b>	Nicht-Qualifizierte elektronische Signatur
<b>PKI</b>	Public Key Infrastructure
<b>PP</b>	Protection Profile – Schutzprofil
<b>QES</b>	Qualifizierte elektronische Signatur
<b>SAK</b>	Signaturanwendungskomponente
<b>SAR</b>	Security Assurance Requirement – Vertrauenswürdigkeitsanforderungen
<b>SHA</b>	Secure Hash Algorithm

<b>SF</b>	Security Function - Sicherheitsfunktion
<b>SFP</b>	Security Function Policy - Politik der Sicherheitsfunktion
<b>SFR</b>	Security Functional Requirement - Funktionale Sicherheitsanforderungen
<b>SIS</b>	Secure Internet Service
<b>ST</b>	Security Target – Sicherheitsvorgaben
<b>TI</b>	Telematikinfrastruktur
<b>TLS</b>	Transport Layer Security
<b>TOE</b>	Target of Evaluation – Evaluierungsgegenstand (EVG)
<b>TSC</b>	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
<b>TSF</b>	TOE Security Functionality – EVG-Sicherheitsfunktionalität
<b>TSL</b>	Trust-service Status List
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	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: Verfahrensdokumentation 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<sup>8</sup> <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/zertifizierungsberichte>
- [6] Sicherheitsvorgaben BSI-DSZ-CC-1135-2020, Version 2.4, 07.08.2020, Security Target für secunet konnektor 2.0.0 (eHealth Konnektor PTV3), secunet Security Networks AG
- [7] Evaluierungsbericht, Version 1.0, 14.08.2020, Evaluation Report - Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH, Dateiname: 1135\_1157\_ETR\_200814\_v10.docx (vertrauliches Dokument)
- [8] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Version 1.5.4, 17.03.2020, 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 2.0, 02.07.2020, secunet Security Networks AG

<sup>8</sup>speziell

- 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)

Inklusive Errata: Errata Version 1.0, 13.08.2020, Errata der Bedienungsanleitung Version 2.0, Produkttypversion: 3.6.0-2 (PTV3) Firmwareversion: 3.5.0, secunet Konnektor 2.0.0 und 2.1.0

[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, eHealthExperts, Version 2.0.0, Stand 11.10.2019, Dateiname: konnektor-rest-doc-2-0-0.pdf (auf Anfrage beim Hersteller)

[d] Security Guidance Fachmodulentwicklung; eHealthExperts; v.1.3; 10.06.2020; Dateiname: Security Guidance Fachmodulentwicklung\_v1.3.pdf

[11] Konfigurationsliste für den EVG (vertrauliche Dokumente)

200629\_ALC\_CMS\_Modularar-Konnektor\_NK-Implementierung\_v2.0.xlsx

1135\_1044-V3\_1157\_1128-V2\_References\_secunet\_konnektor v2.4.pdf

Konfigurationsliste (ALC\_CMS.4), Version 3.18, Datei: ALC\_CMS\_eHX\_v3.1.xls

Konfigurationsliste (ALC\_CMS), Regulatory Affairs Document, S.I.E, 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

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm ", April 1992

[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
- [RFC4492] 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. Donnerhackle, 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

[13] Referenzen auf Anwendungsstandards:

- [gemSpec\_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec\_Kon], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 5.4.0, 26.10.2018 zuzüglich der Errata 1 bis 6 für den PTV3 Konnektor
- [gemSpec\_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastuktur [gemSpec\_Krypt], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.16.0, 02.03.2020

[gemSpec\_Net] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec\_Net], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 1.17.0, 02.03.2020

[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

- [14] [ARC\_AK] eHealthExperts EHX Group, Security Architecture (ADV\_ARC), Anwendungskonnektor, Version 2.5, 12.05.2020 (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 -komponenten: 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