Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1044-2019

zu

secunet konnektor 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-1044-2019 (*)

secunet konnektor 2.0.0

von	secunet Security Networks AG
PP-Konformität:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, V1.5, 27.04.2018, BSI-CC-PP-0097-2018
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_FLR.2, ALC_TAT.1, AVA_VAN.5

SOGIS
Recognition Agreement
für Komponenten bis
EAL 4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 ergänzt um Interpretationen des Zertifizierungsschemas und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 5 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) evaluiert. CC und CEM sind ebenso als Norm ISO/IEC 15408 und ISO/IEC 18045 veröffentlicht.

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

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

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

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

Bonn, 25. Januar 2019

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Joachim Weber
Fachbereichsleiter

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

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

2 Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

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

- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht.
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation/CEM), Version 3.1 [2] auch als Norm ISO/IEC 18045 veröffentlicht.
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]

3. Anerkennungsvereinbarungen

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

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

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

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen 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 http://www.sogisportal.eu eingesehen werden.

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

Dieses Zertifikat fällt unter die Anerkennung nach den Regeln des SOGIS-MRA, d.h. bis einschließlich der Komponenten nach CC Teil 3 EAL 4. Die Evaluierung beinhaltete die Komponente AVA_VAN.5, die nicht nach den Regelungen des SOGIS-MRA anerkannt ist. Für die Anerkennung ist hier die jeweilige EAL 4 Komponente maßgeblich.

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 ratifiiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis

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

einschließlich EAL 2 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP).

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite 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 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts secunet konnektor 2.0.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 7. Dezember 2018 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.

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 25. Januar 2019, ist gültig bis 24. Januar 2024. 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 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

Weidenauer Straße 223-225
57076 Siegen

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 der secunet konnektor 2.0.0. Der EVG ist als Netzkonnektor Bestandteil des Konnektors in der deutschen Telematikinfrastruktur. Der Konnektor ist darauf ausgerichtet, durch Weiterentwicklung und Update im Feld über den Umfang der Online-Rollout Stufe 1 hinaus für weitere Versionen, wie den Online-Produktivbetrieb Stufe 1 (OPB1), nachgenutzt zu werden.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Schutzprofil [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_FLR.2, ALC_TAT.1, AVA_VAN.5.

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 Sicherheits-funktionalität des EVG umgesetzt:

Sicherheitsfunktionalität des EVG	**Thema**
VPN-Client	Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei 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 Telematikinfrastruktur-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen Netzen der Leistungserbringer betreffen, nutzen den VPN-Tunnel zum Sicheren Internet Service.
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 das 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, welche den Betriebszustand an der Außenhaut des Konnektors anzeigt.
Netzdienste: Zertifikatsprüfung	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

Sicherheitsfunktionalität des EVG	Thema
	Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch vermöge 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 eine Möglichkeit, die eigene Integrität zu überprüfen. 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. Im Falle einer Software-Aktualisierung wird dieselbe Bootkette durchlaufen, aber vom Bootloader das neue SW Image geprüft und geladen. Schlägt die Prüfung der Integrität fehl, so wird ein Neustart des EVG durchgeführt und dann das ursprüngliche SW Image geladen.
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 dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG verhindert darüber hinaus den Abfluss von geheimen Informationen, 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 gematik-Spezifikation [14].
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 zur Verfügung steht. Der Administrator kann die Version des Update-Paketes prüfen und den Updateprozess anstossen. Die

Sicherheitsfunktionalität des EVG	Thema
	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 läuft ab, aber vom Bootloader wird das neue Update-Paket 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 die 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 Administrator-Schnittstelle 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 der gematik-Spezifikation [14] 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 Clientsystemen 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 ggf. benötigte Betriebszustände wiederherzustellen. Die TLS-Verbindungen werden vom Anwendungskonnektor gemanagt und je nach Anwendungsfall eingerichtet.

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 Kapiteln 3.3, 3.4 und 3.5 dar.

Dieses Zertifikat umfasst die in Kapitel 8 beschriebene Konfiguration des EVG

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

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

2. Identifikation des EVG

Der Evaluierungsgegenstand (EVG) heisst:

secunet konnektor 2.0.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	FW	secunet konnektor 2.0.0: bestehend aus Netzkonnektor Version: 2.0.36 und Anwendungskonnektor Version: 1.0.7	2.0.0	Entweder wird die Software im Zuge der Fertigung auf die Hardware (Version: 2.0.0) gebracht und über eine sichere Lieferkette ausgeliefert oder als Software-Update Paket über KSR verteilt
2	DOC	secunet(konnektor, Modularer Konnektor Version 2.0.0, Bedienhandbuch, Für Administratoren und Benutzer, secunet Security Networks AG SHA-256 Prüfsumme: A0C54C2872742D3A390449B8B7B38CFE3E8EAAAA3B445E3D30c257A44222DEED	1.04, 19.11.2018	Die Handbücher können auf der Herstellerwebseite heruntergeladen werden.
3	DOC	secunet(konnektor v2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG SHA-256 Prüfsumme: D67338E98E6DEE817902856A01F846D645B5A50BE79E5E16A51B356ABD1466E6	1.7, 10.10.2018	Die Handbücher können auf der Herstellerwebseite heruntergeladen werden.

Tabelle 2: Auslieferungsumfang des EVG

Die Beschreibung der sicheren Lieferkette sowie die Anweisungen an den Nutzer, wie die Einhaltung der sicheren Lieferkette überprüft werden kann, findet sich in [9].

Die Version des EVG kann über die grafische Benutzeroberfläche ermittelt werden. Eine Beschreibung dazu findet sich in [10], Kapitel 6.2.5.6. 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.

3. Sicherheitspolitik

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

- Trusted Path / geschützte Kanäle,
- Dynamischer Paketfilter,
- Netzdienste,
- Stateful Packet Inspection,
- Selbstschutz,
- Administration,
- kryptographische Basisdienste.

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.AK: Korrekte Nutzung des EVG durch Anwendungskonnektor,
- 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.

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

5. Informationen zur Architektur

Eine Übersichtsbeschreibung des allgemeinen Architekturkonzepts des Konnektors finden sich in den Sicherheitsvorgaben [6], Kapitel 1.3.4.

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

Tests des Herstellers

Das Testkonzept sieht drei verschiedene Testansätze vor, wobei automatisierte Tests die Mehrheit aller Tests stellen:

- Automatisiert: eine XML Datei spezifiziert Testfunktionen und sogenannte Test-Evaluatoren, die von der Testumgebung ausgeführt werden sollen.
- Manuell: Die einzelnen Testschritte werden manuell durch den Tester ausgeführt.
- Code Review: Der Hersteller erbringt in Einzelfällen den Nachweis, dass Sicherheits-funktionen korrekt implementiert sind, durch Source Code Analyse der relevanten Code Bereiche.

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

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 aus-zuführenden 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.

Alternative Test Umgebung NWTU

Der Hersteller hat neben der oben beschriebenen Testumgebung eine zweite 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.

Testergebnis

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

Tests des Evaluators

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.

Unabhängiger Testansatz

Die Herstellertests wurden an der Testumgebung des Herstellers wiederholt. Diese Testumgebung wurde auch bei unabhängigen Evaluatortests zum Aufsetzen einer Netzwerkinfrastruktur verwendet (zum Beispiel zur Simulation der VPN-Konzentratoren oder Servern der TI). Dabei wurden zusätzliche Testwerkzeuge, wenn nötig, eingesetzt.

Test Konfiguration

Die Evaluatoren haben alle Sicherheitsfunktionen des EVG an der finalen Produktversion oder an einer Debug-Version des EVG durchgeführt. Im Rahmen der unabhängigen Tests des Evaluators, sowie der durchgeführten Penetrationstests, wurden die im Folgenden aufgeführten Testbereiche abgedeckt:

- Tests aller TSFI durch automatisierte Testausführungen (fwVersion 2.0.35),
- Tests aller TSF durch manuelle Testausführungen (fwVersion 2.0.35),
- Source Code Analyse, durchgeführt durch die Evaluatoren (fwVersion 2.0.36),
- Statische Source Code Analyse der Java Implementierung durch Tools (fwVersion 2.0.35),
- RFC-Analyse der TLS Implementierung (fwVersion 2.0.35),
- RFC-Analyse der VPN Implementierung (fwVersion 2.0.35),
- Last-Tests der VPN Verbindungen (Aufbau und Abbau des Kanals), (fwVersion 2.0.35 und 2.0.36)
- Tests der TLS Implementierung durch die TLS Testumgebung von SRC (fwVersion 2.0.35)
- Tests der VPN Implementierung durch die VPN Testumgebung von SRC (fwVersion 2.0.35)
- Netzwerk-Pentests an allen Netzwerkschnittstellen und an den relevanten Netzwerkprotokollen (fwVersion 2.0.34 und Wiederholung ausgewählter Testfällen an fwVersion 2.0.35),
- Analyse and Tests der FW Regeln (fwVersion 2.0.36).

Die in den Klammern angegebenen Versionsangaben bestimmen die jeweils getestete Konfiguration durch den Parameter fwVersion. In den Fällen, bei denen die Tests nicht an der finalen Version, sondern an fwVersion 2.0.34 oder 2.0.35 durchgeführt wurden, hat der Evaluator jeweils die Unterschiede zwischen den Versionen 2.0.34, 2.0.35 und 2.0.36 betrachtet und im Hinblick auf die durchgeführten Tests bewertet. Der Evaluator kam dabei zu dem Schluss, 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 anderen Änderungen am EVG nicht beeinflusst wird. Die in den Vorgängerversionen erhaltenen Testergebnisse sind daher auch für die finale EVG Konfiguration gültig.

Für Testzwecke wurde der Prüfstelle eine sogenannte „Extended Release“ Variante des EVG zur Verfügung gestellt. Dadurch wurden Untersuchungen des EVG insbesondere für den AVA Aspekt vereinfacht oder überhaupt erst möglich gemacht (z. B. durch Zugriff auf das Betriebssystem des EVG).

Die Extended Release Variante soll dabei neben den nötigen Anpassungen möglichst gering von der finalen Produktversion abweichen. Der Evaluator hat dazu die

Unterschiede zwischen EVG und Extended Release Variante untersucht und kommt zu dem Schluss, dass die Unterschiede zwischen EVG und Extended Release Variante des Konnektors keinen Einfluss auf die damit erhaltenen Testergebnisse haben.

Testauswahl für Unabhängige Tests

Neben der Wiederholung von Herstellertests wurden vom Evaluator eigene Testfälle erstellt. Diese Testfälle decken die folgenden Funktionalitäten ab:

- Netzwerk Filteregeln,
- Reguläre Nutzung des NTP Servers,
- EVG Selbstschutz,
- EVG Administration.

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

Penetrationstests

Alle Konfigurationen des EVG, die von dieser Evaluierung abgedeckt sind, wurden getestet. Insgesamt wurden keine Abweichungen zwischen erwartetem und tatsächlichem Verhalten des EVG festgestellt; insbesondere war kein Angriffsszenario, welches einen Angreifer mit hohem Angriffspotential (high attack potential) voraussetzt, erfolgreich. Diese gilt unter der Annahme, dass alle Maßnahmen, die vom Hersteller an den sicheren Betrieb gestellt sind, auch umgesetzt werden.

Penetrationstest-Ansatz

Im ersten Schritt wurden öffentlich bekannte Schwachstellen anhand von CVE-Listen, Fachliteratur und wissenschaftlichen Veröffentlichungen zusammengetragen. Für die jeweiligen Angriffspfade wurde bewertet, ob der EVG in seiner Betriebsumgebung anfällig für diese Schwachstelle ist.

Die Diskussion dazu beginnt mit einer Übersicht der relevanten Informationen sowie der für die Analyse berücksichtigten Evaluierungsdokumente. Anschließend wurden die für kryptografischen Operationen relevanten SFRs diskutiert. Als Ergebnis wurde festgestellt, dass alle verwendeten Schlüssel, die vom EVG verarbeitet werden, ausreichend Entropie besitzen und die Ableitung des Schlüsselmaterials für die genutzten Operationen geeignet ist.

Im zweiten Teil der Schwachstellenanalyse wurden die Ergebnisse einzelner Evaluationstätigkeiten zusammengetragen. Die jeweiligen Nachweisedokumente der CC wurden dabei schon im Rahmen der Evaluierung einzelner CC Aspekte auf mögliche Schwachstellen für den EVG untersucht. Es wurden bei der Analyse der Nachweisdokumente keine Anzeichen für ausnutzbare Schwachstellen gefunden.

Des Weiteren fanden im dritten Teil der Schwachstellenanalyse die einzelnen Punkte des JIL Dokumentes [4] als Anhaltspunkt für mögliche weitere Schwachstellen im EVG Eingang in die Untersuchung. Alle möglichen Angriffsszenarien gegen einen authentischen operativen EVG wurden analysiert.

Die nächste Diskussion in Teil IV behandelt den Lebenszyklus des Konnektors. Dabei wurde anhand der einzelnen Phasen des Lebenszyklus (Entwicklung, Produktion, Installation, Personalisierung und operativer Betrieb) begründet, warum mögliche Schwachstellen für den vorliegenden EVG nicht ausnutzbar sind.

In Teil V der Schwachstellenanalyse wurde diskutiert, auf welcher technischen Ebene (Hardwareebene oder verschiedene Protokollschichten der externen Schnittstellen) ein Angreifer Ansatzpunkte für einen Angriff finden kann und warum letztendlich keine Angriffe auf den einzelnen Ebenen erfolgreich durchführbar sind.

In Teil VI wurden gezeigt, dass für die im Schutzprofil [8] definierten Assets keine weiteren Schwachstellen existieren, die nicht schon durch die vorangegangenen Analysen betrachtet wurden.

Test Konfiguration

Die Evaluatoren haben die Sicherheitsvorgaben für die Betriebsumgebung in der Schwachstellenanalyse berücksichtigt.

Test Konfiguration für Penetrationstests im Vergleich zur finalen EVG Konfiguration

Neben der finalen Version des EVG wurde für die Testdurchführung eine Debug-Version des Konnektors verwendet, die zusätzliche Testfunktionalität aufweist. Diese zusätzliche Funktionalität ermöglichte die Durchführung bestimmter Tests (z. B. Verifikation der sicheren Löschung von Schlüsseln), die im finalen Konnektor nicht durchführbar sind (und auch nicht durchführbar sein dürfen).

Der Evaluator kommt zu dem Schluss, dass die Unterschiede zwischen finalem EVG und Debug-Version keinen Einfluss auf die damit erhaltenen Testergebnisse haben und die an der Debug-Version gewonnen Testergebnisse auch für den finalen EVG gültig sind.

Getestete Angriffsszenarios

Die folgenden Angriffsszenarien wurden am EVG durchgeführt bzw. durch Design und Code Analyse bewertet:

- Ausnutzen von Schwachstellen in der Paketfilter Konfiguration des EVG,
- Ausnutzen von Schwachstellen in der Implementierung allgemeiner Netzwerkprotokolle,
- Ausnutzen von Schwachstellen in der Implementierung der TLS oder IPsec/IKE Protokolle

8. Evaluierte Konfiguration

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

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 Vertrauens-würdigkeitsstufe EAL 5 erweitert durch Vorgaben der Zertifizierungsstelle für Komponenten höher EAL 5 verwendet.

Für die Analyse des Zufallszahlengenerators wurde AIS 20 angewandt (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_IMP.1, ADV_TDS.3, ALC_FLR.2, ALC_TAT.1, AVA_VAN.5

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, V1.5, 27.04.2018, BSI-CC-PP-0097-2018 [8]
- Funktionalität: PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform / erweitert EAL 3 mit Zusatz von ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_FLR.2, ALC_TAT.1, AVA_VAN.5

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2. Ergebnis der kryptographischen Bewertung

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

Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Anwendungs-standard	Bemer-kungen
Authen-tizität	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
Authen-tisierung	RSA Signaturgenerierung mit Unterstützung 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
Schlüs-selaus-hand-lung	Diffie-Hellman Schlüssel-aushandlung (DH) für VPN (IPsec IKEv2)	[HaC] (DH) [RFC3526] (DH Group) [RFC7296] (IKEv2)	DH: group 14, 2048 Bit Exponent-Länge ≥ 384Bits	[gemSpec_Krypt], Kp. 3.3.1	FCS_CKM.2/NK.IKE

Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Anwendungs-standard	Bemer-kungen
	Diffie-Hellman (DH) und Elliptic Curve Diffie-Hellman Schlüsselaus-handlung (ECDH) für TLS	[RFC4346] (TLS v1.1) [RFC5246] (TLS v1.2) [RFC3268] (DHE_RSA) [RFC4492] (EC-DHE_RSA) [RFC3526] (DH Group 14)	DH: group 14, 2048 Bit, Exponent-Länge = 2048 Bit ECDH: Schlüssellänge entspricht der verwendeten elliptischen Kurve P-{256,384} [FIPS186-4] und brainpoolP{256, 384}r1 [RFC 7027]	[gemSpec_Krypt], Kp. 3.3.1	FCS_CKM.1/NK.TLS
Schlüs-selab-leitung	HMAC Berechnung für VPN (PRF) PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	[FIPS180-4] (SHA) [RFC2404] (HMAC) [RFC7296] (IKEv2)	128, 256	[gemSpec_Krypt], Kp. 3.3.1	FCS_COP.1/NK.HMAC
	KDF für TLS v1.1 und v1.2	[RFC4346] (TLS v1.1) [RFC5246] (TLS v1.2) [FIPS180-4] (SHA), [RFC1321] (MD5), [RFC2104] (HMAC),	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_CKM.1/NK.TLS
Integrität	HMAC Berechnung und Verifikation für VPN HMAC mit SHA-1, SHA-256	[FIPS180-4] (SHA) [RFC2104] (HMAC) [RFC2404] (HMAC-SHA-1 für ESP) [RFC4868] (HMAC-SHA-2 für IPsec) [RFC7296] (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) [RFC2104] (HMAC) [RFC4346] (TLSv1.1) [RFC5246] (TLSv1.2)	160, 256, 384	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.HMAC

Zweck	Kryptografische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Anwendungs-standard	Bemer-kungen
Vertrau-lichkeit	Symmetrische Ver- und Entschlüsselung mit ESP und für VPN AES-CBC (OID 2.16.840.1.101.3.4.1.42)	[FIPS197] (AES) [RFC3602] (AES-CBC) [RFC4303] (ESP) [RFC4301] (IPsec)	256	[gemSpec_Krypt], Kp. 3.3.1	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
	Symmetrische Ver- und Entschlüsselung für TLS AES-{128, 256} in CBC	[FIPS197] (AES) [RFC3602] (AES-CBC) [RFC3268] (AES-TLS mit DH) [RFC4492] (AES-TLS mit ECDH)	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.AES
Authenti cated Encrypti on	AES-{128, 256} in GCM für TLS v1.2	[FIPS197] (AES) [RFC3268] (AES-TLS) [SP800-38D] (GCM) [RFC5289] (AES-GCM-TLS) [RFC5116] (AEAD)	128, 256	[gemSpec_Krypt], Kp. 3.3.2	FCS_COP.1/NK.TLS.AES
Sichere Verbin-dung	TLS v1.1 und v1.2	[RFC4346] (TLSv1.1) [RFC5246] (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)	[RFC4301] (IPsec) [RFC4303] (ESP) [RFC7296] (IKEv2) [SMD3_NK] [SMD3_MS]		[gemSpec_Krypt], Kp. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS

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 Richtline BSI TR-02102' (https://www.bsi.bund.de) entnommen werden.

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

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Sicherheitsniveau mehr als 100 Bit	Bemerkungen
Authentizität	GPG RSA Signaturverifikation mit Encoding RSASSA-PKCS1-1.5 und SHA-512	[RFC4880] (OpenPGP) [RFC8017] (RSA), [FIPS180-4] (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	[RFC8017] (RSA), [FIPS180-4] (SHA)	4096	Ja	Signaturverifikation von UpdateInfo.xml und FirmwareGroupInfo.xml FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update

Tabelle 4: Kryptografische Funktionen des EVG (Update)

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 Risikomanagement-prozess für das IT-System berücksichtigt werden.

Zertifizierte Aktualisierungen des EVG sollten verwendet werden, sofern sie zur Verfügung stehen. Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen. In der Zwischenzeit sollte der Risikomanagementprozess für das IT-System, in dem der EVG eingesetzt wird, prüfen und entscheiden, ob noch nicht zertifizierte Aktualisierungen und Patches zu verwenden sind oder zusätzliche Maßnahmen getroffen werden müssen, um die Systemsicherheit aufrecht zu erhalten.

11. Sicherheitsvorgaben

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

12. Definitionen

12.1. Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CEM	Common Methodology for Information Technology Security Evaluation - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik
cPP	Collaborative Protection Profile
DH	Diffie-Hellman
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
eGK	Elektronische Gesundheitskarte
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
EVG	Evaluierungsgegenstand
gSMC-K	Sicherheitsmodul für den Konnektor
HBA	Heilberufsausweis
HMAC	Keyed-Hash Message Authentication Code
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
MD5	Message-Digest Algorithm 5
NK	Network connector
PKI	Public Key Infrastructure

PP	Protection Profile - Schutzprofil
SAR	Security Assurance Requirement – Vertrauenswürdigkeitsanforderungen
SHA	Secure Hash Algorithm
SF	Security Function - Sicherheitsfunktion
SFP	Security Function Policy - Politik der Sicherheitsfunktion
SFR	Security Functional Requirement - Funktionale Sicherheitsanforderungen
SIS	Secure Internet Service
ST	Security Target – Sicherheitsvorgaben
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation - Evaluierungsgegenstand
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität
TSL	Trust-service Status List
VPN	Virtual Private Network
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[7] https://www.bsi.bund.de/AIS

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

[6] Sicherheitsvorgaben BSI-DSZ-1044-2019, Version 1.4, 4. November 2018, secunet konnektor 2.0.0, secunet Security Networks AG

[7] Evaluierungsbericht, Version 1.1, 7. Dezember 2018, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH (vertrauliches Dokument)

[8] Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, V1.5, 27.04.2018, BSI-CC-PP-0097-2018

[9] Dokumente zur sicheren Lieferkette:

- secunet(konnektor v2.0.0, Hinweise zur sicheren Lagerung und Lieferkette, secunet Security Networks AG, Version 1.7, 10. Oktober 2018

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen inklusive JIL Dokument und CC Supporting Dokument
- 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)

- secunet(konnektor v2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 1.7, 10. Oktober 2018

[10] secunet(konnektor, Modularer Konnektor Version 2.0.0, Bedienhandbuch, Für Administratoren und Benutzer, secunet Security Networks AG, Version 1.04, 19. November 2018

[11] Konfigurationsliste für den EVG (vertrauliche Dokumente)

- 181122_ALC_CMS_Modularar-Konnektor_NK-Implementierung_v1.1.xlsx
- eHealthExperts EHX Group, ALC_CMS.4, Konfiguartionsliste, Version 1.2, 14. September 2018
- ALC_CMS_eHx_v1.9.ods
- Konfigurationsliste (ALC_CMS), Regulatory Affairs Document, S.I.E, Rev# 200, 11. Juni 2018

[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

[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 deut-schen CC-Zertifizierungsschema, Version 0.97, 16. August 2018

[SMD3_MS] IPsec-RFCs - MAY_SHOULD Anforderungen, secunet(konnektor, Ver-sion 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_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.10.0, 14.05.2018

[TR03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für die eCard-Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Technische Arbeitsgruppe TR-03116, 30.01.2014 (Version 3.18)

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 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