Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-1128-V3-2021

zu

secunet konnektor 2.1.0, Version 4.1.3:2.1.0

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-1128-V3-2021 (*)

secunet konnektor 2.1.0
Version 4.1.3:2.1.0

von	secunet Security Networks AG
PP-Konformität:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, Version 1.6.6, BSI-CC-PP-0097-V2-2020-MA-01 vom 15.04.2021
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_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5 und ALC_FLR.2

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.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bonn, 16. Juli 2021

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Joachim Weber
Fachbereichsleiter

L.S.

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....6
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....11
1. Zusammenfassung....12
2. Identifikation des EVG....15
3. Sicherheitspolitik....17
4. Annahmen und Klärung des Einsatzbereiches....17
5. Informationen zur Architektur....17
6. Dokumentation....18
7. Testverfahren....18
8. Evaluierte Konfiguration....20
9. Ergebnis der Evaluierung....20
10. Auflagen und Hinweise zur Benutzung des EVG....25
11. Sicherheitsvorgaben....26
12. Definitionen....26
13. Literaturangaben....28
C. Auszüge aus den Kriterien....32
D. Anhänge....33

A. Zertifizierung

1. Vorbemerkung

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

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

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

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

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

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

2. Grundlagen des Zertifizierungsverfahrens

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

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und - Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN ISO/IEC 17065
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (CC-Produkte) [3]
- BSI Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (CC-Stellen) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation/CC), Version 3.1[4] [1], auch als Norm ISO/IEC 15408 veröffentlicht

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

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

3 Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019,Bundesgesetzblatt I S. 1365

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

3. Anerkennungsvereinbarungen

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

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

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

Die Basisanerkennungsstufe schließt die Common Criteria (CC) Vertrauenswürdigkeitsstufen EAL 1 bis EAL 4 ein. Für Produkte im technischen Bereich "smartcard and similar devices" ist eine SOGIS Technical Domain festgelegt. Für Produkte im technischen Bereich "HW Devices with Security Boxes" ist ebenfalls eine SOGIS Technical Domain festgelegt. Des Weiteren erfasst das Anerkennungsabkommen auch erteilte Zertifikate für Schutzprofile (Protection Profiles) basierend auf den Common Criteria.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen, Details zur Anerkennung sowie zur Historie des Abkommens können auf der Internetseite https://www.sogis.eu eingesehen werden.

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

Dieses Zertifikat fällt 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 Komponenten AVA_VAN.5 die nicht nach den Regelungen des SOGIS-MRA anerkannt sind. 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 ratifiziert. Es deckt CC-Zertifikate ab, die auf sog. collaborative Protection Profiles (cPP) (exact use) basieren, CC-Zertifikate, die auf Vertrauenswürdigkeitsstufen bis einschließlich EAL 2 oder die Vertrauenswürdigkeitsfamilie Fehlerbehebung (Flaw Remediation, ALC_FLR) basieren und CC Zertifikate für Schutzprofile (Protection Profiles) und für collaborative Protection Profiles (cPP).

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

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite https://www.commoncriteriaportal.org eingesehen werden.

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

Dieses Zertifikat fällt unter die Anerkennungsregeln des CCRA-2014, d.h. Anerkennung bis einschließlich CC Teil 3 EAL 2+ 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 2.1.0, Version 4.1.3:2.1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-1044-V2-2019. Für diese Evaluierung wurden bestimmte Ergebnisse aus dem Evaluierungsprozess BSI-DSZ-CC-1044-V2-2019 wiederverwendet.

Die Evaluation des Produkts secunet konnektor 2.1.0, Version 4.1.3:2.1.0 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 27. Mai 2021 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[5].

Der Sponsor und Antragsteller ist: secunet Security Networks AG.

Das Produkt wurde entwickelt von: secunet Security Networks AG.

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

5. Gültigkeit des Zertifizierungsergebnisses

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

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

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

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des Produktes regelmäßig überprüfen zu lassen. Aus diesem Grunde sollte der Hersteller das zertifizierte Produkt im Rahmen des Assurance Continuity-Programms des BSI überwachen lassen (z.B. durch eine Neubewertung oder eine Re-Zertifizierung). Insbesondere wenn

[5] Information Technology Security Evaluation Facility

Ergebnisse aus dem Zertifizierungsverfahren in einem nachfolgenden Evaluierung- und Zertifizierungsverfahren oder in einer Systemintegration verwendet werden oder wenn das Risikomanagement eines Anwenders eine regelmäßige Aktualisierung verlangt, wird empfohlen, die Neubewertung der Widerstandsfähigkeit regelmäßig, z.B. jährlich vorzunehmen.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 16. Juli 2021, ist gültig bis 15. Juli 2026. Die Gültigkeit kann im Rahmen einer Re-Zertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,
3. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, bei denen die Zertifizierung des Produktes aber von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

6. Veröffentlichung

Das Produkt secunet konnektor 2.1.0, Version 4.1.3:2.1.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[6] secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Deutschland

B. Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1. Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist ein Softwareprodukt, bestehend aus dem Netzkonnektor. 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 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.5 und ALC_FLR.2.

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 6.2 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als CC Teil 2 erweitert.

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

Sicherheitsfunktionalität des EVG	**Thema**
VPN-Client	Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service (SIS) bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut, hierbei wird IKEv2 unterstützt.
Informationsflusskontrolle	Regelbasiert nutzen alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel. Nur Informationsflüsse, die vom Konnektor initiiert wurden sowie Informationsflüsse von Clientsystemen in Bestandsnetze dürfen den VPN-Tunnel in die Telematikinfrastruktur benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale TI-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen Netzen der Leistungserbringer betreffen, nutzen den VPN-Tunnel zum Sicheren Internet Service (SIS).
Dynamischer Paketfilter	Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird als Informationsflusskontrolle modelliert. Die Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt und können vom Administrator für den SIS verwaltet werden.
Netzdienste: Zeitsynchronisation	Der EVG führt bei bestehender Verbindung zur TI in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand am Gehäuse 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 Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate

Sicherheitsfunktionalität des EVG	Thema
	kryptographisch mittels der aktuell gültigen TSL und CRL.
Stateful Packet Inspection	Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“. Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird.
Selbstschutz: Speicheraufbereitung	Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session-keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben mit Nullen. Der EVG speichert medizinische Daten nicht dauerhaft. Ausnahmen sind die Speicherung von Daten während ihrer Ver- und Entschlüsselung; auch diese werden sobald wie möglich nach ihrer Verwendung gelöscht.
Selbstschutz: Selbsttests	Der EVG bietet seinen Benutzern die Möglichkeit, 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. 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.
Selbstschutz: Schutz von Geheimnissen, Seitenkanal-resistenz	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 wirkungsvoll, etwa die session-keys der VPN-Verbindung oder zu schützende Daten der TI und der Bestandsnetze.
Selbstschutz: Sicherheits-Log	Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation.
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 EVG dass ein Software Update-Paket zur Verfügung steht. Der Administrator kann die Version des Update-Paketes prüfen und den Updateprozess anstoßen. Die Automatische Installation von Software Updates wird vom EVG nicht unterstützt. Im Falle einer Software-Aktualisierung wird der EVG neu gestartet und dieselbe Bootkette wie in der Sicherheitsfunktion „Selbstschutz“ beschrieben, abgelaufen. Das neue Update-Paket wird vom Bootloader auf Integrität geprüft und bei

Sicherheitsfunktionalität des EVG	Thema
	erfolgreicher Prüfung geladen. Das alte Image wird vom EVG verworfen. Schlägt die Prüfung der Integrität fehl, so wird das Update-Paket verworfen und ein Neustart des EVG durchgeführt mit dem das ursprüngliche SW Image geladen wird. Durch die Prüfung des Update-Pakets analog zum regulären Boot-Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können.
Kryptographische Basisdienste	Der Konnektor implementiert Kryptographische Basisdienste für den Aufbau von sicheren VPN-Verbindungen zu den VPN-Konzentratoren der TI und des SIS.
TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen	Der Netzkonnektor stellt dem Anwendungskonnektor die Dienste zum Aufbau eines TLS-Kanals zur Verfügung. TLS wird auch zur Absicherung der Administratorschnittstelle verwendet. Die kryptographischen Basisdienste für TLS des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des TLS-Kanals). Zertifikate die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen, werden vom Netzkonnektor entsprechend den Anforderungen in [gemSpec_Kon] interpretiert. Der EVG prüft insbesondere, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist enthalten ist. Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen werden X.509-Zertifikate verwendet. Entsprechende Zertifikate für das Clientsystem können vom EVG erzeugt werden. Der EVG bietet dem Administrator eine sichere Schnittstelle zum exportieren dieser X.509-Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel. Zertifikate für Clientsysteme können auch vom EVG über die gesicherte Management-Schnittstelle durch den Administrator importiert werden, um ggfls. 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 6 dargestellt.

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in den Kapiteln 3.3, 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 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 2.1.0, Version 4.1.3:2.1.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1.	HW	secunet konnektor 2.1.0 Hardware für Rechenzentrums-konnektor (RZK) (nicht Teil des EVG)	Hardware Version: 2.1.0 (RZK[7]) BIOS FW Version: 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 oder TCOS Security Module Card - K Version 2.0 Release 1	Die gSMC-Ks sind in der Konnektor-Hardware verbaut.
3.	SW	secunet konnektor 2.1.0 Firmware	EVG-Version: 4.1.3:2.1.0 bestehend aus: Netzkonnektor-Version: 4.1.3[8] Anwendungskonnektor-Version: 3.1.5	Die Software wird im Zuge der Fertigung auf die Hardware gebracht und über eine sichere Lieferkette ausgeliefert. Es besteht zusätzlich die Möglichkeit, dass die Software als Software-Update-Paket über KSR verteilt werden kann.
4.	SW	AMTS, NFDM und ePA Fachmodul Firmware (nicht Teil des EVG)	NFDM-Fachmodul: secunet Fachmodul NFDM 2.1.2 AMTS-Fachmodul: secunet Fachmodul AMTS 2.1.2 ePA-Fachmodul: secunet Fachmodul ePA 3.1.5	Die Fachmodule sind integraler Bestandteil des Anwendungskonnektor-Image.

[7] Bei der Variante Rechenzentrumskonnektor handelt es sich um zwei Einbox-Konnektoren, die (ohne Einbox-Gehäuse) in einem 19 Zoll Gehäuse mit einer Höheneinheit verbaut sind.

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

Nr	Typ	Identifier	Version	Auslieferungsart
5.	DOC	Associated guidance documentation	secunet(konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Bedienungsanleitung, Für Administratoren und Benutzer, Version 3.0, 22.04.2021, Secunet Security Networks AG SHA256: AEA5D6ECBD25AAC76E97303A8B7647E3FD78D17AB3C4FB2285C1491CE9295995 Errata Version 1.0, 06.05.2021, Errata der Bedienungsanleitung Version 3.0, Produkttypversion: 4.8.2-0 (PTV4) Firmwareversion: 4.1.3, secunet Konnektor 2.0.0 und 2.1.0 SHA256: 8A9CA5FB0CFA99320C3DF20EF7D1B89A1AB25A41CF6FE99292A36E696910969E	Die Handbücher können auf der Herstellerwebseite heruntergeladen werden.
6.	DOC		secunet(konnektor v2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer SHA256: 5D7B1F22E54EC1C59D1E74A3EDC0D8207C919576F54B9EBF7BF360B9D39E5F8E	
7.	DOC		Konnektor Management API-Dokumentation, eHealthExperts, Version 3.0.2, Stand 21.01.2021 SHA256: 5392C0D794F9FEB43C36A269CBA791F5B4F5EB4894C30053E6DEBD10ED5E531A	Die REST-API Spezifikation der Management-Schnitt-stelle wird im Handbuch erwähnt und nur auf Anfrage durch den Hersteller gezielt ausgeliefert.
8.	DOC		Security Guidance Fachmodulentwicklung; eHealthExperts; v.1.5; 19.04.2021 SHA256: 8CF0B092EC51D3CAC35C8A7B36FFB810CD4F618309B79281295153C2FEF61F77	Die Security Guidance Fachmodulentwicklung wird nur intern den Fachmodul-Entwicklern zur Verfügung gestellt.

Tabelle 2: Auslieferungsumfang des EVG

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

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

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

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

Die im Konnektor verbauten gSMC-Ks können anhand der Identifikationsnummer (ICCSN) ermittelt werden, siehe [10] [a] Kapitel 9.3.1. Die ICCSN der Karte besteht aus 20 Stellen. Die elfte Stelle der ICCSN gibt dabei an, ob im secunet konnektor 2.1.0 Karten (gSMC-K) vom Typ STARCOS (Wert 0 oder 2) oder TCOS (Wert 1) verbaut sind (siehe [10] [a] Tabelle 19 bzw. [10] [a] Tabelle 21).

3. Sicherheitspolitik

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

4. Annahmen und Klärung des Einsatzbereiches

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

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

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 Gegen-stand dieser Evaluierung waren. Die Sicherheitsfunktionen des EVG sind:

- VPN-Client
- Dynamischer Paketfilter mit zustandsgesteuerter Filterung
- Netzdienste (Zeitsynchronisation und Zertifikatsprüfung)
- Stateful Packet Inspection
- Selbstschutz (Speicheraufbereitung, Selbsttests, Schutz von Geheimnissen und Seitenkanalresistenz, Sicherheits-Log)

- Administration (Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung und Software Update)
- Kryptographische Basisdienste
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Entsprechend dem EVG-Design werden dieses Sicherheitsfunktionen von folgenden Subsys-temen umgesetzt:

- Konnektor-Basissystem
- Subsystem VPN
- TLS-Basis Subsystem
- Konnektormanagement Subsystem
- Laufzeitumgebung Subsystem

6. Dokumentation

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

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

7. Testverfahren

Zur Bestätigung aller Sicherheitsfunktionen des EVG wurden folgende Methoden angewendet:

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

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

In den Fällen, bei denen die Tests nicht an der finalen Version, sondern an anderen Versionen durchgeführt wurden, wurde eine Analyse der Änderungen am EVG zwischen getesteter und finaler Version anhand der bereitgestellten Beschreibungen des Herstellers und insbesondere des Source-Codes durchgeführt. Dabei konnte festgestellt werden, dass eine Wiederholung der Tests an der finalen EVG-Version nicht notwendig ist, da die jeweils getestete Sicherheitsfunktion sich nicht geändert hat und durch die Änderungen am EVG nicht beeinflusst wird. Die an den jeweiligen Vorversionen erhaltenen Testergebnisse sind somit vollständig auf die finale EVG-Version 4.1.3 übertragbar.

Bei Tests und Schwachstellenanalyse wurde systematisch das Angreiferpotential “High” (AVA_VAN.5) unterstellt.

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

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

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

Herstellertests

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

Testumgebung ANKE

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.

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 Testergebnisse festgestellt. Es war kein Angriffsszenario, welches einen Angreifer mit hohem Angriffs-potential (high attack potential) 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“[9] als einzige Konfiguration des EVG (siehe [6], Kapitel 1.3).

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

9. Ergebnis der Evaluierung

9.1. CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [7] wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien [1], der Methodologie [2], den Anforderungen des

[9] Konkret: Bei der Variante Rechenzentrumskonnektor handelt es sich um zwei Einbox-Konnektoren, die (ohne Einbox-Gehäuse) in einem 19 Zoll Gehäuse mit einer Höheneinheit verbaut sind.

Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluierungsmethodologie CEM [2] wurde für die Komponenten bis zur Vertrauenswürdigkeitsstufe 5 verwendet. Darüber hinaus wurde die in der AIS 34 [4] definierte Methodologie 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.5 und ALC_FLR.2

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-1044-V2-2019 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden.

Die Evaluierung hat gezeigt:

- PP Konformität: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor, Version 1.6.6, BSI-CC-PP-0097-V2-2020-MA-01 vom 15.04.2021 [8]
- Funktionalität: PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5 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	Implementierungs-standard	Schlüssel-größe in Bit	Anwendungs-standard	Bemer-kungen
Authenti-zität	RSA Verifikation von Signaturen für VPN und TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC8017] (PKCS#1) [FIPS180-4] (SHA)	2048	[gemSpec_Krypt] Kap. 3.3.1 und 3.3.2	FPT_TDC.1/ NK.Zert FPT_TDC.1/ NK.TLS.Zert
	Verifikation von Signaturen der TSL mit RSASSA-PSS	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048	gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/ NK.Zert FPT_TDC.1/N K.TLS.Zert

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
		[RFC-6931] (XMLDSig)			FPT_TDC.1/AK
	Verifikation von Signaturen der CRL mit RSASSA-PKCS1-v1_5 sha256WithRSAEnc-ryption	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048	gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert FPT_TDC.1/AK
Authentisierung	RSA Signatur-Erzeugung mit Unterstützung der gSMC-K und -Verifikation für VPN und TLS sha256withRSAEn-cryption (OID 1.2.840.113549.1.1.11) sha384withRSAEn-cryption (OID 1.2.840.113549.1.1.12) (für TLS) sha512withRSAEn-cryption (OID 1.2.840.113549.1.1.13) (für TLS)	[RFC8017] (RSASSA-PKCS1-v1_5) [FIPS180-4] (SHA)	2048	[gemSpec_Krypt] Kap. 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: Gruppe 14, 2048 Bit Exponenten-Länge 2047 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_CKM.2/NK.IKE
	Diffie-Hellman Schlüsselaushandlung (DH) und Elliptic Curve Diffie-Hellman Schlüsselaushandlung (ECDH) für TLS	[HaC] (DH) [SEC1] (ECDH) [RFC-5246] (TLS v1.2) [RFC-3268] (DHE_RSA) [RFC-4492] (EC-DHE_RSA) [RFC-3526] (DH Gruppe 14)	DH: Gruppe 14, 2048 Bit, Exponentenlänge = 2048 Bit ECDH: Schlüssellängen entsprechend der verwendeten elliptischen Kurven P-{256,384} [FIPS 186-4] und brainpoolP{256, 384}r1 [RFC 7027]	[gemSpec_Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Schlüsselableitung	HMAC Berechnung für VPN (PRF) PRF-HMAC-SHA-1, PRF-HMAC-SHA-256	IANA] mit [RFC-8247#2.2] [FIPS 180-4] (SHA) [RFC-2404] (HMAC) [RFC7296] (IKEv2)	128, 256	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.HMAC
	Schlüsselableitung für TLS v1.2	[RFC-5246] (TLS v1.2) [FIPS-180-4] (SHA) [RFC-2104] (HMAC)	128, 256	[gemSpec_Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS
Schlüsselgenerierung	RSA Schlüsselgenerierung im X.509- und PKCS#12-Format	[RFC4055] (sup. [RFC5280]) [RFC7292] (PKCS#12) [FIPS186-4] (Method B.3.3)	2048	TR 03116-1	FCS_CKM.1/NK.Zert
Integrität	HMAC Berechnung und Prüfung für VPN HMAC mit SHA-1, SHA-256	[FIPS180-4] (SHA) [RFC-2104] (HMAC) [RFC-2404] (HMAC-SHA-1 mit ESP) [RFC-4868] (HMAC-SHA-2 mit IPsec) [RFC-7296] (IKEv2)	160, 256	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.HMAC
	HMAC Berechnung und Prüfung für TLS HMAC mit SHA-{1, 256, 384}	[FIPS180-4] (SHA) [RFC-2104] (HMAC) [RFC-5246] (TLSv1.2)	160, 256, 384	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.HMAC

Zweck	Kryptografische Funktion	Implementierungsstandard	Schlüsselgröße in Bit	Anwendungsstandard	Bemerkungen
Vertraulichkeit	Symmetrische Ver- und Entschlüsselung mittels ESP für VPN-Kommunikation AES-CBC (OID 2.16.840.1.101.3.4.1.42)	[FIPS 197] (AES) [RFC-3602] (AES-CBC) [RFC-4303] (ESP, IPSec) [RFC-4301] (IPsec)	256	[gemSpec_Krypt], Kap. 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], Kap. 3.3.2	FCS_COP.1/NK.TLS.AES
Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	AES-{128, 256} in GCM Mode 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], Kap. 3.3.2	FCS_COP.1/NK.TLS.AES
Sichere Kanäle	TLS v1.2	[RFC-5246] (TLS v1.2) [SMD3_AK] [SMD3_MS_AK]	-	[gemSpec_Krypt], Kap. 3.3.2	FTP_ITC.1/NK.TLS FTP_TRP.1/NK.Admin
	VPN (IKEv2) mit zertifikatbasierter Authentisierung	[RFC-4301] (IPsec) [RFC-4303] (ESP) [RFC-7296] (IKEv2) [SMD3_NK] [SMD3_MS]	-	[gemSpec_Krypt], Kap. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS

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 mittels RSASSA-PKCS1-1.5 unter Anwendung von SHA-512	[RFC-4880] (OpenPGP) [RFC-8017] (RSA) [FIPS 180-4] (SHA)	2048	Ja	Signaturverifikation des Firmware-Updates FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
	RSA Signaturverifikation mittels RSASSA-PSS unter Anwendung von SHA-256	[RFC-8017] (RSA) [FIPS 180-4] (SHA)	4096	Ja	Signaturverifikation der UpdateInfo.xml und FirmwareGroupInfo.xml FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update

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

AMTS Arzneimitteltherapiesicherheit

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
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
eGK	Elektronische Gesundheitskarte
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
EVG	Evaluierungsgegenstand – Target of Evaluation (TOE)
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
NFDM	Notfalldatenmanagement
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 (EVG)
TSC	TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functionality – EVG-Sicherheitsfunktionalität

TSL Trust-service Status List

VPN Virtual Private Network

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

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

[6] Sicherheitsvorgaben BSI-DSZ-CC-1128-V3-2021, Version 1.8, 26.04.2021, Security Target für secunet konnektor 2.1.0, secunet Security Networks AG

[7] Evaluierungsbericht, Version 1.2, 27.05.2021, Evaluation Report - Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH, Dateiname: 1044-V4_1128-V3_ETR_210527_v12.docx (vertrauliches Dokument)

[8] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.6, 15.04.2021, 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 3.0, 22.04.2021, secunet Security Networks AG

Inklusive Errata: Errata Version 1.0, 06.05.2021, Errata der Bedienungsanleitung Version 3.0, Produkttypversion: 4.8.2-0 (PTV4) Firmwareversion: 4.1.3, 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 3.0.2, Stand 21.01.2021, file name: konnektor-rest-doc-3-0-2.pdf (auf Anfrage beim Hersteller)

[d] Security Guidance Fachmodulentwicklung; eHealthExperts; v.1.5; 19.04.2021; file name: Security Guidance Fachmodulentwicklung_v1.5.pdf

[11] Konfigurationsliste für den EVG (vertrauliche Dokumente)

210322_ALC_CMS_Modularar-Konnektor_NK-Implementierung_v2.4.xlsx

1163_1044-V4_1174_1128-V3_References_secunet_konnektor v2.4.pdf

[10] insbesondere

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)

Konfigurationsliste (ALC_CMS.4), Version 5.4, Datei: ALC_CMS_eHX_v5.4.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], [AES] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[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_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec_Kon], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 5.9.5, 04.12.2020

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.16.2, 05.11.2020

[gemSpec_Net] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik Gesellschaft für Telemati-kanwendungen der Gesundheitskarte mbH, Version 1.17.2, 04.12.2020

[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

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

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

[TR-03157] BSI TR-03157 Konnektor – Prüfspezifikation für das Fachmodul ePA, Technische Richtlinie BSI TR-03157, Version 1.2, 24.07.2019

C. Auszüge aus den Kriterien

Die Bedeutung der Vertrauenswürdigkeitskomponenten und -stufen kann direkt den Common Criteria entnommen werden. Folgende Referenzen zu den CC können dazu genutzt werden:

- Definition und Beschreibung zu Conformance Claims: CC Teil 1 Kapitel 10.5
- Zum Konzept der Vertrauenswürdigkeitsklassen, -familien und -kompomenten: CC Teil 3 Kapitel 7.1
- Zum Konzept der vordefinierten Vertrauenswürdigkeitsstufen (evaluation assurance levels - EAL): CC Teil 3 Kapitel 7.2 und 8
- Definition und Beschreibung der Vertrauenswürdigkeitsklasse ASE für Sicherheitsvorgaben / Security Target Evaluierung: CC Teil 3 Kapitel 12
- Zu detaillierten Definitionen der Vertrauenswürdigkeitskomponenten für die Evaluierung eines Evaluierungsgegenstandes: CC Teil 3 Kapitel 13 bis 17
- Die Tabelle in CC Teil 3 Anhang E fasst die Beziehung zwischen den Vertrauenswürdigkeitsstufen (EAL) und den Vertrauenswürdigkeitsklassen, -familien und -komponenten zusammen.

Die Common Criteria sind unter https://www.commoncriteriaportal.org/cc/ veröffentlicht.

D. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

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

Bemerkung: Ende des Reportes