Company confidential

Evaluation Report

- Evaluation Technical Report (ETR) -

Version:
Version 2.3

Date:
12.02.2026

File name:
1044-V9_ETR_260212_v23.docx

Product:

secunet konnektor 2.0.0 und 2.1.0

Developer:
secunet Security Networks AG

Evaluation Facility:
SRC Security Research & Consulting GmbH,
Emil-Nolde-Straße 7, D-53113 Bonn, Germany,
Phone: +49 (228) 2806-0, Fax: +49 (228) 2806-199

Certification ID:	BSI-DSZ-CC-1044-V9
Evaluators:	see history
Quality assurance:	see history

Document Information

History of changes

Version	Date	Autor	Approved	Changes
Version 0.9	2020-08-12	msc	-	Initial Version based on the report from BSI-DSZ-CC-1044-V2-2019.
Version 1.0	2020-08-14	msc	bk	QA version. This version integrates the changes of the QA.
Version 1.1	2021-05-07	msc, dae	bk	Updated version based on the report from BSI-DSZ-CC-1044-V3-2020 resp. -1128-V2-2020.
Version 1.2	2021-05-27	msc	bk	Editorial changes, references updated
Version 1.3	2022-02-25	msc, dae	bk	Updated version based on the report from BSI-DSZ-CC-1044-V4-2021 resp. -1128-V3-2021.
Version 1.4	2022-03-11	msc	bk	Editorial changes, references updated
Version 1.5	2022-03-17	msc	bk	Editorial changes after comments from BSI
Version 1.6	2022-07-29	dae	bk	Updated version based on the report from BSI-DSZ-CC-1044-V5-2022 resp. -1128-V4-2022.
Version 1.7	2022-08-10	msc	bk	Editorial changes, references updated
Version 1.8	2023-08-25	msc	dae	Updated version based on the report from BSI-DSZ-CC-1044-V6-2022 resp. -1128-V5-2022.
Version 1.9	2024-06-21	msc	dds	Updated version for ALC re-evaluation, based on the report from BSI-DSZ-CC-1044-V7-2023 resp. -1128-V6-2023. Includes updates from the maintenance BSI-DSZ-CC-1044-V7-2023-MA-01 resp. resp. -1128-V6-2023-MA-01, e.g. TOE version, document updates etc.
Version 2.0	2025-03-27	msc	dds	Updated version for PTV5 Plus (WR4) konnektor re-evaluation, based on the report from BSI-DSZ-CC-1044-V7-2023-MA-02. RZK and EBK TOEs are now combined in one security target as TOE configurations. HW version 2.0.1 has been removed.
Version 2.1	2025-04-09	msc	dds	Editorial changes. References updated
Version 2.2	2025-04-10	msc	dds	Editorial changes. References updated
Version 2.3	2026-02-12	msc (authorised)	dds	Updated version for PTV6 konnektor re-evaluation, based on the report from BSI-DSZ-CC-1044-V8-2025.

Document Invariants

Name	Invariant (edit here)	Output value
File name and size	calculated automatically	1044-V9_ETR_260212_v23.docx
Current version	Version 2.3	Version 2.3
Date	12.02.2026	12.02.2026
Classification	Company confidential	Company confidential
TOE name (long)	secunet konnektor 2.0.0 und 2.1.0	secunet konnektor 2.0.0 und 2.1.0
TOE name (short)	Konnektor PTV6	Konnektor PTV6
Sponsor (long)	secunet Security Networks AG	secunet Security Networks AG
Sponsor (short)	secunet	secunet
Developer (short)	secunet	secunet
Developer (long)	secunet Security Networks AG	secunet Security Networks AG
Certification ID	BSI-DSZ-CC-1044-V9	BSI-DSZ-CC-1044-V9
Certification body (long)	Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 87, 53175 Bonn, Germany	Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 87, 53175 Bonn, Germany
Certification body (short)	BSI	BSI

Table of contents

Part A

Evaluation

1 Angaben zur Evaluierung

Die aktuelle Evaluierung ist eine Re-Evaluierung auf Basis des Verfahren BSI-DSZ-CC-1044-V8-2025.

Die Änderungen am EVG wurden durch den Hersteller in [CHANGES] dokumentiert. Zusammenfassend ergaben sich für die Evaluierung die folgenden wesentlichen Aspekte:

- Es wurde eine Anpassung des EVG Umfangs im Einklang mit [gemSpec_Kon] durchgeführt, indem für das ePA Fachmodul relevante Teile (VAU- und SGD-Client) entfernt wurden. Dies wurde in der Herstellerdokumentation und den Prüfberichten ebenfalls vollzogen.
- Der Secure-Update-Mechanismus des EVG wurde von RSA-2048bit-Signaturen auf ECDSA (BrainpoolP384r1 mit SHA-384) Signaturen umgestellt. Die entsprechenden Tests des Herstellers und des Evaluators (ATE_IND) berücksichtigen diese Änderung.
- Laut [CHANGES] wurden Komponenten aktualisiert, die kryptographische Dienste an andere interne Komponenten des EVG bereitstellen (OpenSSL und BouncyCastle), sodass im Rahmen der Evaluierung die Kryptokonformität bestätigt wurde, [AVA_CCA]. Des Weiteren wurden im Rahmen der Evaluierung die Auswirkungen auf die Implementierung untersucht, [TLS_Analysis], [VPN_Analysis], [BSI_Liste_analysis], sowie TLS spezifische Tests, [TLS_Tests], durchgeführt, um die sichere Funktionalität zu verifizieren.
- Laut [CHANGES] wurden diverse Komponenten aktualisiert, sodass im Rahmen der Evaluierung die Pentrationstests gemäß [AVA_Testplan] durchgeführt und in [Network_PEN_Testing] dokumentiert wurden.

Die Herstellerdokumentation und Evaluationsergebnisse, welche durch die o.g. Änderungen unbeeinflusst sind, wurden unverändert übernommen und gelten auch für das aktuelle Verfahren weiterhin.

Dieser ETR behandelt das Verfahren

- BSI-DSZ-CC-1044-V9, Einboxkonnektor (EBK) und Rechenzentrumskonnektor (RZK), secunet konnektor 2.0.0 und 2.1.0

1.1 Target of Evaluation (TOE)

Target of evaluation (TOE) of this Evaluation Technical Report (ETR) is the product secunet konnektor 2.0.0 und 2.1.0, 6.0.8:2.0.0 resp. 6.0.8:2.1.0 provided by secunet Security Networks AG. The TOE is a pure software TOE consisting of the Netzkonnektor as specified in the protection profile [NK-PP].

The Netzkonnektor includes the security functionality of a firewall and a VPN client as well as a NTP Server, a name service (DNS) and a DHCP service. It also includes the basic functions for establishment of secure TLS connections to other IT products.

The associated guidance is considered part of the TOE:

- secunet(konnektor, Bedienungsanleitung, Für Administratoren und Benutzer, Version 7.4, 23.10.2025, Secunet Security Networks AG, including -

referring to Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025

- secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023
- Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025
- Security Guidance Fachmodulentwicklung; eHealthExperts; v2.0; 25.06.2025

The TOE implements the Security Functionality as listed in Tabelle 1.

Tabelle 2 provides references to documents describing the TSFIs and the TOE Design, including the classifications in SFR-enforcing, SFR-supporting and SFR-non-interfering.

1.2 Evaluierungsgegenstand (EVG)

Der in diesem Evaluation Technical Report (ETR) vorgestellte Evaluierungsgegenstand ist das Produkt secunet konnektor 2.0.0 und 2.1.0, 6.0.8:2.0.0 bzw. 6.0.8:2.1.0 der Firma secunet Security Networks AG. Der Evaluationsgegenstand (EVG) ist ein Softwareprodukt, bestehend aus dem Netzkonnektor nach dem Protection Profile [NK-PP].

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 zugehörige Benutzerdokumentation ist Teil des EVGs:

- secunet(konnektor, Bedienungsanleitung, Für Administratoren und Benutzer, Version 7.4, 23.10.2025, Secunet Security Networks AG, inklusive -

  referenziert Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025
- secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023
- Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025
- Security Guidance Fachmodulentwicklung; eHealthExperts; v2.0; 25.06.2025

Der Netzkonnektor setzt folgende Sicherheitsfunktionalitäten um:

Sicherheitsfunktionalität des NK als Teil des EVG	**Adressiertes 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.

Sicherheitsfunktionalität des NK als Teil des EVG	Adressiertes Thema
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 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

Sicherheitsfunktionalität des NK als Teil des EVG	Adressiertes Thema
	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 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 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 das ein Software-Update durchgeführt werden kann. 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, aber vom Bootloader wird das neue Update-Paket auf Integrität geprüft und bei erfolgreicher Prüfung geladen. Das

Sicherheitsfunktionalität des NK als Teil des EVG	Adressiertes Thema
	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 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 Clientsystemen können vom EVG erzeugt werden. Der EVG bietet dem Administartor 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: Übersicht der Sicherheitsfunktionalität NK

Die folgende Liste verweist auf Dokumente, welche die TSFIs und das TOE Design einschließlich der Klassifizierung in SFR-enforcing, SFR-supporting und SFR-non-interfering wiedergeben.

Kurzbezeichnung	Vollständige Referenz

[FSP]	Funktionale Spezifikation secunet konnektor 2.0.0, 2.0.1 und 2.1.0, Version v5.2, 28.03.2025
[TDS_NK]	secunet(konnektor Version 2.0.0, 2.0.1 und 2.1.0, Technical Design Specification (ADV_TDS), secunet Security Networks AG, Version 2.25, 04.03.2025
[TDS_AK]	TOE-Design, Anwendungskonnektor, eHealthExperts GmbH, Version 2.12, 26.06.2025

Tabelle 2: Dokumente zu den TSFIs und zum TOE Design

1.3 Beteiligte Personen

Die folgenden Personen waren am Evaluierungsprozess beteiligt:

Applicant:	secunet Security Networks AG	
Certification Body	Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 87, 53175 Bonn, Germany Herr Sinan Civelek	
Evaluation Facility / Evaluators:	SRC Security Research & Consulting GmbH Emil-Nolde-Straße 7 53113 Bonn	
	Name[2]	**Role and task**[3]
	Mark Schall (msc)	Head evaluator, Project Management Evaluation: ASE, AGD_ADV, ADV, ALC (editorisch), ATE, AVA, AVA (CCA), VPN-/Zert-Analyse, AVA (CVE analysis) QA: AVA (Penetration testing), ATE, ALC, TLS-Analyse, TSL-Tests
	David Seim (dds)	Evaluation: ATE, ALC (incl. Audit) QA: ASE, AGD_ADV, ADVAVA (CVE-Analyse)
	Sven-Martin Hühne (smh)	Evaluation: ALC (incl. Audit)
	Daniel Ginster (dgi)	Evaluation: ALC (incl. Audit)
	Tim Hirschberg (thi)	Evaluation: AVA (Penetration testing)
	Matthias Heuft (mh)	Evaluation: TLS-Analyse, TSL-Tests QA: VPN-/Zert-Analyse, AVA (CCA)
	Joshua Huberti (joh, in vocational adjustment)	Evaluation: ASE, AGD_ADV, AVA (Penetration testing), AVA (CCA)

Tabelle 3: Beteiligte Personen

[2] Die Kürzel für die Namen in Klammern werden in den Einzelprüfberichten eingesetzt

[3] Nur Tätigkeiten im Rahmen der aktuellen Evaluierung, BSI-DSZ-CC-1044-V9

Für eine Liste aller involvierten Personen – insbesondere für die beteiligten Evaluatoren – siehe auch die Tabelle am Ende von Kapitel 11.

1.4 Zeitlicher Ablauf der Evaluierung

Der zeitliche Ablauf der Evaluierung war wie folgt:

Date / Time period	Action
NK-Evaluierung	*BSI-DSZ-CC-1044-2019*
04.07.2017	*Kick-Off Meeting*
14.02.2018	*Abstimmungs Workshop*
16.03.2018	*PRE-ADV und DEL-Workshop*
23.01.2018	*Site visit at the development site in Berlin, Germany*
24.01.2018	*Site visit at the development site in Dresden, Germany*
31.01.2018 – 01.02.2018	*Site visit at the development site in Essen, Germany*
10.04.2018 - 11.04.2018	*Site visit at the production site in Lustenau, Austria*
10.07.2018	*ADV-Workshop*
11.07.2018	*ATE-Workshop*
25.10.2018	*Workshop Diverses*
16.11.2018	*AVA Workshop 1*
05.12.2018	*AVA Workshop 2*
December 2018	*Completion of the Vulnerability Analysis*
06.12.2018	*Submission of ETR v1.0 to BSI*
07.12.2018	*Submission of ETR v1.1 to BSI*
NK Re-Evaluierung	*BSI-DSZ-CC-1044-V2*
10.09.2019	*Completion of the Vulnerability Analysis*
18.09.2019	*Workshop (IAR and AVA)*
02.10.2019	*Submission of ETR v1.2 to BSI*
PTV3 Evaluierung	*BSI-DSZ-CC-1044-V3 und BSI-DSZ-CC-1128-V2*
23.01.2020	*ADV Workshop*
18.02.2020	*ATE Workshop*
29.04.2020	*AVA Workshop Teil 1 (Telefonkonferenz)*
14.05.2020	*AVA Workshop Teil 2 (Telefonkonferenz)*
28.05.2020	*AVA Workshop Teil 3 (Telefonkonferenz)*
31.07.2020	*Completion of the Vulnerability Analysis and Testing*
14.08.2020	*Submission of ETR v1.0 to BSI*

Date / Time period	Action
PTV4 Evaluierung	*BSI-DSZ-CC-1044-V4 und BSI-DSZ-CC-1128-V3*
03.09.2020	*KickOff*
11.12.2020	*ADV Workshop (Telefonkonferenz)*
19.02.2021	*ATE Workshop (Telefonkonferenz)*
19.03.2021	*AVA Workshop Teil 1 (Telefonkonferenz)*
16.04.2021	*AVA Workshop Teil 2 (Telefonkonferenz)*
30.04.2021	*Abstimmungstelko (Abschlussbesprechung AVA)*
30.04.2021	*Abschluss der Schwachstellenanalyse und Tests*
07.05.2021	*Submission of ETR v1.1 to BSI*
27.05.2021	*Submission of ETR v1.2 to BSI*
PTV5 Evaluierung	*BSI-DSZ-CC-1044-V5 und BSI-DSZ-CC-1128-V4*
06.07.2021	*KickOff*
14.09.2021	*ADV Workshop (Telefonkonferenz)*
11.10.2021	*ATE Workshop (Telefonkonferenz)*
07.12.2021	*AVA Workshop (Telefonkonferenz)*
18.02.2021	*Abschluss der Schwachstellenanalyse und Tests*
25.02.2022	*Submission of ETR v1.3 to BSI*
11.03.2022	*Submission of ETR v1.4 to BSI*
17.03.2022	*Submission of ETR v1.5 to BSI*
PTV5 WR1 Evaluierung	*BSI-DSZ-CC-1044-V6 und BSI-DSZ-CC-1128-V5*
24.05.2022	*KickOff*
15.07.2022	*Abschluss der Schwachstellenanalyse und Tests*
29.07.2022	*Submission of ETR v1.6 to BSI*
10.08.2022	*Submission of ETR v1.7 to BSI*
PTV5 WR1 Maintenance	***BSI-DSZ-CC-1044-V6-MA-01 und BSI-DSZ-CC-1128-V5-MA-01***
21.11.2022	*Zertifizierung abgeschlossen*
PTV5 Plus (WR3) Evaluierung	***BSI-DSZ-CC-1044-V7-2023 und BSI-DSZ-CC-1128-V6-2023***
29.09.2022	*KickOff, Teil 1*
26.01.2023	*KickOff, Teil 2*
10.05.2023	*Alle Standort-Audits abgeschlossen*

Date / Time period	Action
25.08.2023	*Abschluss der Schwachstellenanalyse und Tests*
25.08.2023	*Auslieferung des ETR v1.8 ans BSI*
Maintenance (ohne Prüfstellenbeteiligung)	***BSI-DSZ-CC-1044-V7-2023-MA-01 und BSI-DSZ-CC-1128-V6-2023-MA-01***
ALC Re-Evaluation	***BSI-DSZ-CC-1044-V7-2023-MA-02 und BSI-DSZ-CC-1128-V6-2023-MA-02***
19.10.2023	*KickOff (Telefonat mit dem Zertifizierer)*
27.10.2023	*Auditdurchführung am neuen Standort*
21.06.2024	*Auslieferung des ETR v1.9 ans BSI*
PTV5 Plus (WR4) Evaluierung	***BSI-DSZ-CC-1044-V8***
09.09.2024	*KickOff*
06.02.2025	*Abschluss der Schwachstellenanalyse und Tests*
27.03.2025	*Auslieferung des ETR v2.0 ans BSI*
09.04.2025	*Auslieferung des ETR v2.1 ans BSI*
10.04.2025	*Auslieferung des ETR v2.2 ans BSI*
PTV6 Evaluierung	**BSI-DSZ-CC-1044-V9**
24.03.2025	KickOff
24.07.2025	Alle Standort-Audits abgeschlossen
19.11.2025	Abschluss der Schwachstellenanalyse und Tests
12.02.2026	Auslieferung des ETR v2.3 ans BSI

Tabelle 4: Zeitablauf der Evaluierung

1.5 Prüfgrundlagen

Die Evaluierung basierte auf den folgenden CC Dokumenten:

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

Die Einzelprüfberichte (Single Evaluation Report, SER) führen die angewandten AIS und JIL Dokumente auf. Der Anhang dieses Berichtes verweist zudem auf sämtliche angewandten AIS und JIL Dokumente. Im Rahmen der Evaluierung wurde kein berichtsrelevanter Feststellungsbericht (Observation Report) erstellt.

Der Evaluierung lagen die folgenden Sicherheitsvorgaben zugrunde:

[ST] Security Target für secunet konnektor 2.0.0 und secunet konnektor 2.1.0, Version 3.3, 05.02.2026, secunet Security Networks AG (BSI-DSZ-CC-1044-V9)

Die Sicherheitsvorgaben des EVG reklamieren eine Übereinstimmung („strict conformance“) zu dem folgenden Schutzprofil:

- Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.7, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Sicherheitsvorgaben wurden gegenüber dem Schutzprofil produktspezifisch ergänzt.

Die Prüfstelle SRC bestätigt, dass die Sicherheitsvorgaben alle Anforderungen des zugrundeliegenden Schutzprofils enthalten.

Die ausgewählte Vertrauenswürdigkeitsstufe des EVG ist

EAL 3 augmented.

Die Augmentierung beinhaltet die Vertrauenswürdigkeitskomponenten **ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5** und **ALC_FLR.2**

1.6 Abgestimmte Vorgehensweisen

Keine.

2 Lieferumfang des EVG

2.1 Übersicht des Auslieferungsverfahrens

	Liefergegenstand	Beschreibung und ggf. zusätzliche Information	Typ	Liefermethode
1	secunet konnektor 2.0.0 und 2.1.0 Hardware für EBK oder RZK (Non TOE)	Hardware Version: 2.0.0 (EBK, BSI-DSZ-CC-1044-V9) 2.1.0 (RZK, BSI-DSZ-CC-1044-V9) BIOS FW Version: CSASR007 (nur EBK), CSASR009, CSASR011	HW	Das Gerät wird über eine sichere Lieferkette dem Endkunden zugestellt.
2	gSMC-Ks (Non TOE)	- STARCOS 3.6 Health SMCK R1 - TCOS Security Module Card - K Version 2.0 Release 1 - STARCOS 3.7 gSMC-K R1 - TCOS Security Module Card – K Version 2.0 Release 2	HW	Die gSMC-Ks sind in der Konnektor Hardware verbaut.
3	secunet konnektor 2.0.0 und 2.1.0 Firmware	TOE Version[4]: 6.0.8:2.0.0 (EBK, BSI-DSZ-CC-1044-V9) 6.0.8:2.1.0 (RZK, BSI-DSZ-CC-1044-V9) bestehend aus Netzkonnektor Version: 6.0.8[5] Anwendungskonnektor Version: 6.0.13	SW	Entweder wird die Software im Zuge der Fertigung auf die Hardware (Version: 2.0.0 bzw. 2.1.0) gebracht und über eine sichere Lieferkette ausgeliefert oder als Software-Update Paket über KSR verteilt.
4	AMTS, NFDM und ePA Fachmodul Firmware (Non TOE)	NFDM-Fachmodul: secunet Fachmodul NFDM 6.0.0 AMTS-Fachmodul: secunet Fachmodul AMTS 6.0.0	SW	Die Fachmodule sind integraler Bestandteil des Anwendungskonnektor-Image
5	Associated guidance documentation	secunet(konnektor, Bedienungsanleitung, Für Administratoren und Benutzer, Version 7.4, 23.10.2025, Secunet Security Networks AG SHA256: 54f39514df12070c39c83f6675fc36	DOC	Die Handbücher können auf der Herstellerwebseite heruntergeladen werden.

[4] Angabe gemäß [ST], Kapitel 1.1

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

	Liefergegenstand	Beschreibung und ggf. zusätzliche Information	Typ	Liefermethode
		b938b12b82b274b6aa95f5030f3627092e		
		secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023 SHA256: ae467b545732b0f0814a3ff2c6771badbb5f3d2dced8851bdfe4161f03f890e3	DOC	
		Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025 SHA256: 647cfbf231dead821362692ae57063f9f43addf28376d08cc282cb18f6d38abb	DOC	Die REST-API Spezifikation der Management-Schnittstelle wird im Handbuch erwähnt und nur auf Anfrage durch den Hersteller gezielt ausgeliefert.
		Security Guidance Fachmodulentwicklung; eHealthExperts; v2.0; 25.06.2025 SHA256: 86d32d69ffd0bec816c3300cc84b67fdc849ca251df8cd30b60aec5791a8763b	DOC	Die Security Guidance Fachmodulentwicklung wird nur intern den Fachmodul-Entwicklern zur Verfügung gestellt.

Ta**belle 5: Liefergegenstände**

Die sichere Lieferkette wird in den folgenden Dokumenten beschrieben:

- secunet(konnektor Version 2.0.0, 2.0.1 und 2.1.0, Hinweise zur sicheren Lagerung und Lieferkette, Version 2.1, 11.05.2023, [ALC_DEL2]
- secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023, [AGD_DEL]

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

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

2.2 Möglichkeit der Identifizierung des EVGs durch den Anwender

Die Version des EVG kann über die grafische Benutzeroberfläche ermittelt werden. Eine Beschreibung dazu findet sich in [AGD], 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 verbaute gSMC-Ks können anhand der Identifikationsnummer (ICCSN) ermittelt werden, siehe [AGD], Kapitel 9.3.1. Die ICCSN der Karte besteht aus 20 Stellen. Die elfte Stelle der ICCSN gibt dabei an, welcher Typ der gSMC-Ks im secunet konnektor 2.0.0 und 2.1.0 verbaut ist (siehe [AGD], Tabelle 19 bzw. Tabelle 21). Siehe auch Kapitel 6.3.

3 Evaluierte Konfiguration

3.1 Beschreibung der evaluierten Konfiguration des EVG

Die evaluierte Konfiguration des EVG ist durch folgende Festlegungen definiert:

- secunet konnektor 2.0.0 und 2.1.0, 6.0.8:2.0.0 und 6.0.8:2.1.0 (BSI-DSZ-CC-1044-V9)
- Die Dokumente
  - secunet(konnektor, Bedienungsanleitung, Für Administratoren und Benutzer, Version 7.4, 23.10.2025, Secunet Security Networks AG, [AGD], inklusive -
  - Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1, Stand 20.08.2025, [REST-API]
  - Security Guidance Fachmodulentwicklung; eHealthExperts; v2.0; 25.06.2025, [FM-SEC]
  - secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023, [AGD_DEL]

Über die Benutzeroberfläche kann der Administrator die Version des EVG auslesen. Die folgende Tabelle beschreibt die evaluierte Konfiguration.

Produktinformation in der Benutzeroberfläche	JSON Parameter "KonnektorVersion"	Wert
Firmware-Version[6]	fwVersion	6.0.8
Anwendungskonnektor-Version	version	6.0.13
Hardware-Version[7]	hwVersion	2.0.0 (BSI-DSZ-CC-1044-V9) 2.1.0 (BSI-DSZ-CC-1044-V9)

Tabelle 6: Evaluierte Konfiguration

3.2 Beschreibung der Testkonfigurationen

<Begin>Erforderliche Übersicht in editierbarer Form nach AIS 19

Zur Bestätigung aller Sicherheitsfunktionen des EVG wurden folgende Methoden angewendet:

- automatisiertes Testen aller TSFI

[6] Diese Versionsnummer erfasst auch die Version des Anwendungskonnektors; insbesondere induziert ein Update des Anwendungskonnektors eine Änderung des Parameters fwVersion. Zur exakten Bestimmung der TOE Version reicht daher die Angabe der fwVersion.

[7] Diese Versionsnummer erfasst auch die BIOS-Version; insbesondere induziert ein BIOS-Update eine Änderung des Parameters hwVersion.

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

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

Bei Tests und Schwachstellenanalyse wurde systematisch das Angreiferpotential “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.
Der folgende Abriss liefert eine Zusammenfassung der Herangehensweise bei der Schwachstellenanalyse:

- Part I: Es wurde sichergestellt, dass alle relevanten Informationen und Dokumente einbezogen wurden. Die "Generic vulnerability guidance" in B.2.1 von [CEM] kam zur Anwendung.
- Part II: Es wurde untersucht, dass die Auslieferung keine ausnutzbaren Schwachstellen hat.
- Part III: In Anlehnung an die Angriffsmethoden aus [JIL AttMeth] wurden Angriffe auf den operativen EVG gewürdigt.
- Part IV: Die Lebenszyklusphasen Entwicklung, Fertigung, Installation, Personalisierung und regulärer Betrieb wurden auf mögliche Schwachstellen untersucht.
- Part V: Identifikation und Bewertung von Angriffspunkten auf verschiedenen technischen Ebenen und Protokollebenen
- Part VI: Schwachstellenanalyse basierend auf den Assets, die im zugrundeliegenden Protection Profile identifiziert sind.

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

<Ende>Erforderliche Übersicht in editierbarer Form nach AIS 19

Die Evaluatoren haben alle Sicherheitsfunktionen des EVG an der finalen Produktversion oder an einer Debug-Version des EVG durchgeführt, siehe dazu Kapitel 3.2.3. 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 6.0.5)
- Tests aller TSF durch manuelle Testausführungen (fwVersion 5.1.2, 5.70.4, 6.0.5)

- Source Code Analyse, durchgeführt durch die Evaluatoren (fwVersion 5.1.2, 6.0.5)
  - mit Analyse der TOE Änderungen, insb. „Laufzeitverlängerung“ in ADV_IMP, [SER_ADV] (fwVersion 5.50.1)
  - mit Analyse der TOE Änderungen, insb. Zufallszahlengenerator-Untersuchung bezüglich der Umsetzung der AIS20, [SER_ADV_RNG] (fwVersion 5.70.4)
- Statische Source Code Analyse der Implementierung durch Tools (fwVersion 5.0.4)
- RFC-Analyse der TLS Implementierung (fwVersion 6.0.5)
- RFC-Analyse der VPN Implementierung (fwVersion 6.0.5)
- Analyse der Zertifikatsdienst Implementierung (fwVersion 6.0.5),
- Last-Tests der VPN Verbindungen (fwVersion 5.0.2 und 5.0.3)
- Tests der TLS Implementierung durch die TLS Testumgebung von SRC (fwVersion 6.0.5)
- Tests der VPN Implementierung durch die VPN Testumgebung von SRC (fwVersion 5.1.2)
  - mit [VPN_ConfChk] (fwVersion 5.50.1)
- Netzwerk-Pentests an allen Netzwerkschnittstellen und an den relevanten Netzwerkprotokollen (fwVersion 5.1.2, 5.70.4, 6.0.3)
- Analyse und Tests der FW Regeln (fwVersion 5.0.3)
  - mit [FW_ConfChk] (fwVersion 5.50.1, 6.0.8)
- Konformitätsprüfung der Implementierung von Kryptoalgorithmen (fwVersion 6.0.5)

Die Evaluatoren haben die Penetrationstests am Prüfgegenstand (EVG) systematisch und unter Berücksichtigung eines Angreifers mit ***High*** Angriffspotential durchgeführt.

Die dabei erhaltenen Testergebnisse entsprechen den erwarteten Ergebnissen.

3.2.1.1 Anmerkung bezüglich der getesteten Versionsstände und der Debug-Version:

Die in den Klammern angegebenen Versionsangaben bestimmen die jeweils getestete Konfiguration durch den Parameter fwVersion, der die EVG Version wie in Tabelle 6 beschrieben festlegt. In den Fällen, bei denen die Tests nicht an der finalen Version, sondern an anderen Versionen durchgeführt wurden, haben die Evaluatoren eine Analyse der Änderungen des EVG zwischen getesteter und finaler Version anhand der bereitgestellten Beschreibungen des Herstellers (siehe [CHANGES]) und insbesondere des Source-Codes durchgeführt. Die Evaluatoren kamen dabei zu dem Schluss, dass eine Wiederholung der Tests an der aktuellen EVG Version nicht notwendig ist, da die jeweils getestete Sicherheitsfunktion sich nicht geändert hat und durch die anderen Änderungen am EVG nicht beeinflusst wird. Die an den jeweiligen Vorversionen erhaltenen Testergebnisse sind vollständig auf die finale Version 6.0.8 übertragbar.

Neben der finalen Produktversion wurde auch eine Debug-Version des EVG zur Durchführung der Test verwendet, siehe dazu Kapitel 3.2.3. 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.

3.2.2 Tests des Herstellers

Die folgende Zusammenfassung wurde aus [SER_ATE], Work Unit [ATE_FUN.1-7], übernommen und ins Deutsche übersetzt.

EVG Test-Konfiguration

Das [ST] beschreibt nur eine einzelne Konfiguration für den EVG. In [ST], Abschnitt 1.3.2 wird die sogenannte "Einbox-Lösung" als einzige Konfiguration des Evaluierungsgegenstandes angegeben.

Anmerkung: Der Rechenzentrumskonnektor setzt auch die Einbox-Lösung im Sinne des [NK-PP] um.

[ATE_FUN], Abschnitt 2.1, beschreibt das entsprechend dem Testkonzept des Herstellers getestete Testobjekt, bestehend aus Netzkonnektor (NK), Anwendungskonnektor (AK). Die verschiedenen Konfigurationen, die in der Herstellerbeschreibung definiert werden, behandeln nur den Einsatz von Testkomponenten in der Testumgebung des EVG aber nicht die Konfiguration des EVG selbst. Das Testobjekt entspricht der Konfiguration des EVG, wie durch die Sicherheitsvorgaben [ST] definiert.

Testansatz

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

- **Automatisiert**: eine XML Datei oder `.feature` Datei spezifiziert Testfunktionen und sogenannte Test-Evaluatoren, die von der Testumgebung ausgeführt werden sollen. Die Testauswahl beinhaltet überwiegend diese automatisierten Tests.
    - z. B. Testfall `TF_AK_PKI_TSL_Datei_Invalide_01_<nr>` (cons10t test engine)
    - z. B. Testfall `TF_SIGN_DOCUMENT_QES_XAdES_OK_01_<nr>` (ConCuTE test engine)
- **Manuell**: Die einzelnen Testschritte werden manuell durch den Tester ausgeführt. Testnachweise können dabei Screenshots der Administratoroberfläche des EVGs oder Auszüge aus den Log-Dateien sein. Auch für manuelle Tests werden vom Tester XML Dateien mit Informationen zum Test und dem Testresultat bereitgestellt.
    - z. B. Testfall `TF_AK_CONF_LOG_01_01`

- **Code Review**: Der Hersteller erbringt in Einzelfällen den Nachweis, dass Sicherheitsfunktionen korrekt implementiert sind, durch Source Code Analyse der relevanten Code Bereiche.
    - z. B. Testfall TF_VPNKEYS_01

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

Testumgebung ANKE mit Testumgebung cons10t

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) inclusive deren Netzwerkfunktionalität.

Die Testlogik ist in einzelnen Test-Modulen enthalten, die für die jeweiligen Testfälle mit unterschiedlichen Parametern aufgerufen und kombiniert werden können. Dabei könne 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.

Das entsprechende Testmodul wird durch eine eindeutige Identifikations-Nummer `id` referenziert, die in einem Element `testfall/testmodule` der XML-Spezifikation des Testfalls (oder eines anderen Test-Modules) angegeben wird. Die Testumgebung kann das zugehörige Test-Modul anhand der Identifikations-Nummer ermitteln und durch eine `execute()` Methode ausführen. Analog wird der jeweilige Test-Evaluator mittels unabhängiger Identifikations-Nummer identifiziert und durch die `evaluate()` Methode eingebunden.

Der Evaluator hat die Testfallimplementierung in [ATE_IMP] untersucht und den oben beschriebenen Ansatz nachvollzogen. Die Testlogik ist jeweils durch Aufrufen eines Test-Moduls mittels `execute()` Methode realisiert. Die Prüfung des Testergebnisses gegen den erwarteten Wert wird durch den Aufruf eines Evaluator-Moduls mittels `evaluate()` Methode umgesetzt. Dabei sind die einzelnen Test- und Evaluator-Module unabhängig voneinander. Generische Evaluator-Module, wie zum Beispiel ein Modul zum Vergleichen von Strings gegen einen bestimmten Wert, werden in einer Vielzahl von Testfällen verwendet.

Testumgebung ANKE mit Testumgebung ConCuTE

ConCuTE ist eine alternative Test-Engine, die sich auf die ANKE-Testumgebung stützt, aber verschiedene Testpläne in Form von so genannten Feature-Dateien implementiert. Bei den Feature-Dateien handelt es sich um menschenlesbare Textdateien, die von der ConCuTE-Testengine interpretiert werden. Die Feature-Dateien sind in [ATE_FEATURE] referenziert.

Auszug aus PIN_Operationen.feature

```
# Testfälle zu EnablePin
  @AFO_TIP1-A_5487 @AFO_TIP1-A_5486
  Testfallgruppe: [TF_ENABLEPIN_OK_<gruppe>_<nr>] Aufruf der Operation EnablePin - OK ("<cardtype>",
"<pintyp>")
    Vorbedingung: In Slot 1 von Kartenterminal T1 steckt die Karte "<smartcard>" vom Typ "EGK" und
wird vom Konnektor verauskunftet
    * Der Aufrufparameter CardHandle wird mit GetCards für die gesteckte Karte "<smartcard>"
ermittelt
    * Der Aufrufparameter PinTyp ist "<pintyp>"
    * Das Testsystem hat den CETP-Server CETP-1 für den Empfang von CARD Ereignissen am Konnektor
registriert

    Testdurchführung: Der EnablePin-Request wird mit den angegebenen Aufrufparametern ausgeführt

    Ergebnis: Es liegt kein gematik-SOAP-Fault vor
    * Die EnablePinResponse ist schemavalide
    * Der Status-Result der EnablePinResponse ist "OK"
    * Der PinResult der EnablePinResponse ist "OK"
    * Das Kartenterminal T1 hat die Meldung "PIN-Schutz 0x0B<anw> 0x0Beinschalten0x0FPIN.eGK:"
angezeigt
    * Der Konnektor hat das Ereignis CARD/PIN/ENABLE_STARTED an den CETP-Server CETP-1 versendet
    * Der Konnektor hat das Ereignis CARD/PIN/ENABLE_FINISHED an den CETP-Server CETP-1 versendet

    Parameter:
      | gruppe | nr | cardtype | smartcard                          | pintyp     | anw              |
      | 01     | 01 | eGK G2   | ehc-nfdm-G2-mrpin-nfd-deactivated  | MRPIN.NFD  | Notfalldaten     |
      | 01     | 02 | eGK G2   | ehc-nfdm-G2-mrpin-dpe-deactivated  | MRPIN.DPE  | Pers.Erklärungen |
      | 01     | 03 | eGK G2   | ehc-gdd-G2-mrpin-gdd-deactivated   | MRPIN.GDD  | PIN GDD          |
      | 02     | 01 | eGK G2.1 | ehc-nfdm-G21-mrpin-nfd-deactivated | MRPIN.NFD  | Notfalldaten     |
      | 02     | 02 | eGK G2.2 | ehc-nfdm-G21-mrpin-dpe-deactivated | MRPIN.DPE  | Pers.Erklärungen |
      | 02     | 03 | eGK G2.1 | ehc-gdd-G21-mrpin-gdd-deactivated  | MRPIN.GDD  | PIN GDD          |
      | 02     | 04 | eGK G2.1 | ehc-amts-G21-mrpin-deactivated     | MRPIN.AMTS | Medikationsdaten |
```

Tabelle 7: Beispiel einesa ConCuTE Test-Falls

Das Beispiel in Tabelle 7 spezifiziert die Testfälle TF_ENABLEPIN_OK_01_01 bis TF_ENABLEPIN_OK_02_04. Text in <> Klammern (z.B. <Kartentyp>) sind Platzhalter, die aus der Parametertabelle am Ende des Beispiels gefüllt werden. Jede Zeile der Parametertabelle definiert einen Testfall mit seinem Satz von Parametern.

Der Inhalt des Testfalls wird von der Test-Engine (unter Verwendung regulärer Ausdrücke) interpretiert und die Test-Engine entsprechend eingestellt und ausgeführt.

Die Semantik dieses Satzes hängt von der Implementierung der Testmaschine ab, bezieht sich aber idealerweise auf das, was in natürlicher Sprache gesagt wird. Dies ist eine Weiterentwicklung des ANKE-Konzepts zur Interpretation von XML-Dateien, die sowohl die Testspezifikation (in natürlicher Sprache) als auch die Testimplementierung enthalten. Das XML wird durch vordefinierte Sprachkonstrukte ersetzt, die automatisch von der Test-Engine interpretiert werden.

Die AK-Funktionalität wird hauptsächlich mit ConCuTE getestet. Der NK-Teil wird mit cons10t und NWTU-Tests geprüft.

Alternative Test Umgebung NWTU

Der Hersteller hat neben den oben beschriebenen Testumgebungen eine weitere Testumgebung für die Ausführung bestimmter Testfälle bereitgestellt. In [NWTU], Abschnitt 1 heißt es dazu:

> "In diesem zusätzlichen Testaufbau wurden netzwerknahe Testszenarien ausgelagert, deren Automatisierung in ConS10t nicht im vorgeben Zeitrahmen hätten umgesetzt werden können",

d.h., diese alternative Netzwerktestumgebung (*network test environment*, NWTU) 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 und bestehen im Wesentlichen aus drei Unterfunktionen, die nacheinander aufgerufen werden. Die Funktionen signalisieren unabhängig voneinander ob sie erfolgreich durchlaufen wurden:

`custom_set_up()`: Optionale testspezifische Vorbereitungen.

`custom_run()`: Umsetzung der Testfall-Logik

`custom_follow_up()`: Überführung der Testumgebung in den Ausgangszustand; Zurücksetzen der durch custom_set_up() erfolgten Änderungen.

Nach jeder Testausführung wird eine Logdatei erstellt, die das jeweilige Testergebnis PASSED, FAILED oder ABORTED enthält.

Testergebnisse

Die Evaluatoren bestätigen, dass die Übereinstimmung von erwartetem Verhalten des EVG (entsprechend der Designbeschreibungen der Assurance Klasse ADV) und tatsächlichem Testergebnis für die untersuchten Testfälle geprüft wurde.

Die erwarteten Testergebnisse sind in der Testbeschreibung in unterschiedlicher Art und Weise enthalten. In der Regel werden die Ergebnisse in den Logdateien der automatisierten Tests aufgeführt. Bei manuellen Tests werden vom Hersteller diverse Nachweise, wie Logs oder Screenshots, die bei der Testdurchführung vom Tester aufgenommen wurden, bereitgestellt. Wenn der Testfall eine Analyse des Source Codes beinhaltet, besteht das Testergebnis aus der Angabe der relevanten Codestellen.

Im Falle automatisierter Tests wird durch die Testumgebung selbst bewertet ob der Testfall erfolgreich durchlaufen wurde oder nicht (Test-Evaluatoren). Bei manuellen Tests muss diese Bewertung der Tester auf Basis von Vorgaben selbst vornehmen. Die Testfälle mittels Source Code Analyse implizieren eine erfolgreiche Testausführung, da entdeckte Fehler im Code zu einem Bugfix im Rahmen des Entwicklungsprozesses führen.

Für die Bearbeitung der relevanten ATE Work Units wurde eine Samplingstrategie zugrunde gelegt, wie in [ATE_FUN.1-2] beschrieben wird. Der Evaluator hat für die Untersuchung der vom Hersteller bereitgestellten Testfälle die in [ATE_FUN.1-2] festgelegte Testauswahl verwendet und keine Testfälle festgestellt, für die das Testergebnis FAILED lautet.

Generelle Bewertung des Hersteller Testkonzeptes sowie der Testaufwände

Der Testansatz des Herstellers ist das direkte Testen der SFRs. Diese SFRs sind wiederum auf die sicherheitsrelevanten Schnittstellen (TSFIs) des EVGs abgebildet. Die einzelnen Testfälle sind direkt aus den Anforderungen in [gemProdT_Kon] abgeleitet. 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 [ST] 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 [FSP] 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.

Die Testumgebung wird für den EVG vorkonfiguriert ausgeliefert. Unterschiedliche Testsetups sind in der Testumgebung enthalten und werden mit der Testfallausführung automatisch geladen. Die Testfälle werden als XML-Dateien angelegt und von der Test-Engine interpretiert. Diese ist in Java implementiert, bzw. durch Linux Shell Scripts oder durch Anweisungen an den Tester.

Die Test-Skripte können direkt mit einem Text-Editor inspiziert und auch direkt aus der Testumgebung heraus ausgeführt werden. Zusätzlich werden Testsuiten zur Verfügung gestellt, die einen ganzen Satz an Testfällen nacheinander ausführen. Die Testskripts für automatisierte Tests werden zusammen mit der Testumgebung gewartet und ausgeliefert. Der entsprechende Source Code der cons10t Test-Module wurde mit [ATE_IMP] bereitgestellt und von den Evaluatoren bei der Analyse der Testpläne berücksichtigt.

Sämtliche Testprotokolle wurden der Prüfstelle in elektronischer Form zur Verfügung gestellt.

3.2.3 Unabhängige Tests des Evaluators

Die folgende Zusammenfassung wurde aus [SER_ATE], Work Unit [ATE_IND.2-11], übernommen und ins Deutsche übersetzt.

Übersicht:

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

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnissen festgestellt.

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

Der Prüfgegenstand war

- secunet konnektor 2.0.0 und 2.1.0, Hardware Version 2.0.0 und 2.1.0, Firmware Version 6.0.8

Das [ST] beschreibt nur eine einzelne Konfiguration für den EVG. In [ST], Abschnitt 1.3.2 wird die sogenannte "Einbox-Lösung" als einzige Konfiguration des Evaluierungsgegenstandes angegeben.

Anmerkung: Der Rechenzentrumskonnektor setzt auch die Einbox-Lösung im Sinne des [NK-PP] um.

[ATE_FUN], Abschnitt 2.1, beschreibt das entsprechend dem Testkonzept des Herstellers geteste Testobjekt, bestehend aus Netzkonnektor (NK), Anwendungskonnektor (AK). Die verschiedenen Konfigurationen, die in der Herstellerbeschreibung definiert werden, behandeln nur den Einsatz von Testkomponenten in der Testumgebung des EVGs aber nicht die Konfiguration des EVG selbst. Das Testobjekt entspricht der Konfiguration des EVG, wie durch die Sicherheitsvorgaben [ST] definiert.

Für Testzwecke wurde jedoch eine sogenannte "Extended Release" Variante des EVG der Prüfstelle 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. Im Folgenden sind die Ergebnisse dieser Untersuchung zusammengefasst:

- Die Kernel Flags sind identisch, bis auf das Setzen der Flags `CONFIG_IKCONFIG` und `CONFIG_IKCONFIG_PROC` in der Extended Release Variante (siehe unten).
- Die Compiler Flags sind identisch.
- Die ausführbaren Dateien des EVG haben in der Extended Release Variante den gleichen Versionsstand.
  - Die Hintergrunddienste, die in beiden Versionen laufen, haben - bis auf die folgenden Ausnahmen - denselben Versionsstand für die Extended Release Variante:
    - Die Kommandozeile des Linux Betriebssystems ist mittels SSH-Verbindung erreichbar (Die NK-Komponente des EVGs auf Port 22 und die AK Komponente des EVG auf Port 2222).
    - Es gibt Remote Desktop Zugriff via VRDP (*VirtualBox Remote Display Protocol*) zur AK Komponente des EVG auf Port 3389.
- Der USB Device Filter ist deaktiviert.
- DNSSEC kann bei Bedarf deaktiviert werden.
- Der flüchtige Speicher ist für den Export von Testnachweisen (Logging) zugänglich.

- Die Kernel Konfiguration kann aus dem `/proc` File System ausgelesen werden. Das ist durch setzten der Flags `CONFIG_IKCONFIG` und `CONFIG_IKCONFIG_PROC` umgesetzt.
- Test and System Tools sind als Binary Files aufrufbar, z. B. `cd`, `cp`, `ls` und weitere Basis-Kommandos; `ip` oder `ifconfig`; `iptables`, `ping`, `traceroute`, `dig`, `conntrack`, `curl`, `tcpdump`, `netstat`, `ipsec status` und `ipsec statusall`, `grep`, `mount`, `find`, `iperf`, `netcat`, `gdb`, `strace`. Diese Binary Files sind inaktiv, wenn sie nicht durch den Benutzer aktiv ausgeführt werden.

Der Evaluator kommt zu dem Schluss, dass die Unterschiede zwischen EVG und Extended Release Variante des Konnektors keinen Einfluss auf die damit erhaltenen Testergebnisse haben, insbesondere nicht auf die funktionalen Tests.

Alle funktionalen Tests konnten am EVG ausgeführt werden. Tests, die dem AVA Aspekt zugeordnet sind, wurden entweder am EVG oder, wenn notwendig, an der Extended Release Variante ausgeführt. Z. B. können Penetrationstests der USB Schnittstelle nur sinnvoll bei aktiviertem USB-Filter ausgeführt werden (EVG). Tests, die Zugriff auf das Betriebssystem benötigen, brauchen dafür eine entsprechende SSH Verbindung (Extended Release)

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

Die Tests sind in [ATE_IND_NK] dokumentiert.

Weiter Testfälle decken die folgenden Funktionalitäten ab:

- Identifikation und Authentisierung
- Zugriffsberechtigungsdienst
- Kartenterminaldienst
- Kartendienst
- Signaturdienst
- Software-Update
- Verschlüsselungsdienst
- Sicherheitsmanagement
- Schutz der TSF
- Sicherheitsprotokollierung
- Remote Admin

Die Tests sind in [ATE_IND_AK] dokumentiert.

Darüber hinaus wurden folgende Aspekte besonders hinsichtlich einer ausreichenden Testabdeckung untersucht:

- Access Rules (FDP_ACF)
- Signaturdirektive
- Verschlüsselungsdirektive
- Dokumentensicherheit
- Fachmodul-API

Die Analysen sind in [ATE_IND_AK] dokumentiert.

Wiederholung der Herstellertests

Alle automatisierten Testfälle der Herstellertestumgebung wurden wiederholt. Die Test-Protokolle mit Test-Logs befinden sich unter [ATE_IND_DEV]. Alle Testfälle wurden erfolgreich durchgeführt (pass).

Die manuellen Herstellertests wurden nicht wiederholt. Manuelle Tests wurden im Rahmen von Work Unit [ATE_IND.2-8] ausgeführt.

Die wiederholten Tests beinhalten neben allen automatisierten Tests entsprechend ATE_COV auch weitere vom Hersteller zur Verfügung gestellte Testfälle. In der Testausführung sind damit alle im Rahmen von ATE_FUN untersuchten Testfälle enthalten.

Abschließendes Urteil für die Evaluator-Aktivitäten

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

3.2.4 Ausgeführte Penetrationstests

Die folgende Zusammenfassung wurde aus [SER_AVA], Work Unit [AVA_VAN.5-10], übernommen und ins Deutsche übersetzt.

Übersicht:

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.

Anmerkung: Das Security Target [ST] claimt entsprechend den Vorgaben des Protection Profiles [NK-PP] die Assurance Komponente AVA_VAN.5. Die Schwachstellenanalyse wurde im Rahmen der Evaluierung **BSI-DSZ-CC-1209-V3** durchgeführt. Das Security Target [ST] der benannten Evaluierung claimt entsprechend den Vorgaben des dort relevanten Protection Profiles [AK-PP] nur die Assurance Komponente AVA_VAN.3. Als Grundlage für die Schwachstellenanalyse wird jedoch sowohl für TOE nach [AK-PP] als auch nach [NK-PP] die Assurance Komponente AVA_VAN.5 angenommen.

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. Die Kategorien entsprechend der "Generic vulnerability guidance" in B.2.1 von [CEM] wurden dabei untersucht. Anschließend wurden die für kryptografische 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 als Anhaltspunkt für mögliche weitere Schwachstellen im EVG Eingang in die Untersuchung. Alle möglichen Angriffsszenarien gegen einen authentischen operativen EVG wurden analysiert. Dabei wurden die Ergebnisse und Erfahrungen der JIWG Arbeitsgruppe wie in [JIL AttMeth] beschrieben berücksichtigt.

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 [PP] definierten Assets keine weiteren Schwachstellen existieren, die nicht schon durch die vorangegangenen Analysen betrachtet wurden.

Zudem verweist der letzte Teil VI der Analyse auf die von der Prüfstelle durchgeführten Penetrationstests.

Test-Konfiguration

Entsprechend [CEM], Paragraph 1565, müssen die Sicherheitsvorgaben für die Betriebsumgebung, wie sie in [ST] definiert werden, in Betracht gezogen werden. 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).

Getestete Angriffsszenarios

Die folgende Tabelle gibt eine Zusammenfassung über die Angriffsszenarien, die am EVG durchgeführt bzw. durch Design und Code Analyse bewertet wurden:

Angriffsszenarios für Penetrationstests	Kurzbeschreibung
AS.1	Ausnutzen von Schwachstellen in der Paketfilter Konfiguration des EVG
AS.2	Ausnutzen von Schwachstellen in der Implementierung allgemeiner Netzwerkprotokolle und der Verarbeitung von Dokumenten im Signaturdienst und Verschlüsselungsdienst
AS.3	Ausnutzen von Schwachstellen in der Implementierung der TLS oder IPsec/IKE Protokolle

Für die damit verbundenen Testaktivitäten wurden detaillierte Prüfberichte erstellt.

Abschließendes Urteil für die Evaluatoraktivitäten:

Insgesamt wurden keine Abweichungen zwischen erwarteten und tatsächlichen Testergebnisse festgestellt. Es war kein Angriffsszenario, welches einen Angreifer mit hohem Angriffspotential (*high attack potential*) voraussetzt, in der Betriebsumgebung, wie sie im Schutzziel [ST] definiert ist, erfolgreich durchführbar. Diese gilt unter der Annahme, dass alle Maßnahmen, die vom Hersteller an den sicheren Betrieb gestellt sind, auch umgesetzt werden.

3.3 Entwicklungs- und Produktionsstandorte

Die folgenden Standorte sind relevant:

#	Bezeichnung des Standorts	Hinweise zu den Standortbegehungen
	Development	
1	secunet Security Networks AG Kurfürstenstraße 58 45138 Essen, Germany	Primary development site: software engineering, testing Die Begehung wurde am 17.06.2025 durchgeführt.
2	secunet Security Networks AG Dresden West: Ammonstrasse 74 01067 Dresden, Germany Dresden Ost Freiberger Straße 37 01067 Dresden, Germany	Secondary development site: Hosting of TOE development systems, Backup Die Begehung wurde am 26.06.2025 durchgeführt.
3	secunet Security Networks AG Alt-Moabit 96 10559 Berlin, Germany	Third development site: TOE development Die Begehung wurde am 25.06.2025 durchgeführt.
4	eHealth Experts GmbH Albrechtstraße 11 10117 Berlin, Germany	Development site of the Anwendungskonnektor, partially Netzkonnektor Die Begehung wurde am 24.06.2025 durchgeführt.
	Production	
5	System Industrie Electronic GmbH Millenium Park 12 A-6890 Lustenau, Austria	Final production step: installing of the TOE onto the physical device. Die Begehung wurde am 24.07.2025 durchgeführt.

Tabelle 8: Entwicklungs- und Produktionsstandorte

Die Common Criteria Vertrauenwürdigkeitsanforderungen aus der Klasse ALC – Life cycle support (hier: ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1) sind für die in Tabelle 8 genannten Standorte erfüllt.

3.4 Erweiterung der Ergebnisse auf andere Konfigurationen

Die Ergebnisse dieser Evaluierung sind nur für den untersuchten EVG secunet konnektor 2.0.0 und 2.1.0 gültig. Ohne eine weiterführende Evaluierung sind die Ergebnisse dieser Evaluierung nicht auf andere Produktversionen übertragbar.

3.5 Besondere Beschränkungen und Ausnahmen

Es gibt keine besonderen Beschränkungen oder Ausnahmen für den EVG.

3.6 Kryptographische Funktionen

Die folgenden kryptografischen Algorithmen werden vom EVG secunet konnektor 2.0.0 und 2.1.0 zur Umsetzung seiner Sicherheitsrichtlinien verwendet:

	Formal dem Netzkonnektor zugeordnet und durch [NK-PP] abgedeckt
	ST Erweiterung für PTV5 (ECC-Migration TLS)
	ST Erweiterung für PTV5-WR1 (ECC-Migration VPN)

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
1	Authentizität	RSA Verifikation von Signaturen für VPN und TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	VPN: 2048 bit TLS: 2048 and 3072 bit	[gemSpec_Krypt] Kap. 3.3.1 und Kap. 3.3.2	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert
2		ECDSA Verifikation von Signaturen für TLS cdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen Kurven für brainpoolP256r1 ([RFC5639]) und NIST P-	[gemSpec_Krypt] Kap. 3.3.1 und Kap. 3.3.2	FPT_TDC.1/NK.TLS.Zert

[8] RSA Schlüssellängen unter 3000 Bits werden gemäß [gemSpec_Kon] bzw. [gemSpec_Krypt] weiterhin unterstützt. In den meisten Fällen erfolgt der Einsatz von RSA-2048 Bit bei Krypto-Operationen über die eingesetzten Karten (gSMC-K, gSMC-KT, SMC-B, HBA, eGK), die sich weiterhin in der Einsatzumgebung des TOEs befinden bzw. vom TOE genutzt werden müssen, um seine Funktionalität zu erbringen. In den Fällen, wo der TOE selbst RSA Schlüssel generiert (z. B. für TLS-Zertifikate), wird ebenfalls gemäß [gemSpec_Krypt] der TOE Zufallszahlengenerator der Klasse DRG.3 (siehe [SER_ADV_RNG]) eingesetzt und Schlüssellängen von mindesten RSA-3072 Bit oder ECC-256 Bit generiert.

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
				256 ([FIPS186-4])		
3		ECDSA Verifikation von Signaturen für VPN ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der Verwendeten elliptischen Kurven für brainpoolP256r1 ([RFC5639])	[gemSpec Krypt] Kap. 3.3.1 und Kap. 5.5	FPT_TDC.1/NK.Zert
4		Verifikation von Signaturen der TSL mit RSASSA-PSS	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA) [RFC-6931] (XMLDSig)	2048 Bit	[gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert FPT_TDC.1/AK
5		Verifikation von Signaturen der CRL mit RSASSA-PKCS1-v1_5 sha256WithRSAEncryption	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec_Krypt], Kap. 3.14	FPT_TDC.1/NK.Zert FPT_TDC.1/NK.TLS.Zert FPT_TDC.1/AK
6	Authentisierung	RSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für VPN und TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) sha384withRSAEncryption (OID 1.2.840.113549.1.1.12) (für TLS) sha512withRSAEncryption (OID 1.2.840.113549.1.1.13) (für TLS)	[RFC-8017] (RSASSA-PKCS1-v1_5) [FIPS 180-4] (SHA)	VPN: 2048 bit TLS: 2048 and 3072 bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.Auth FCS_COP.1/NK.TLS.Auth
7		ECDSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für TLS	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256)	Schlüssellänge entsprechend der verwendeten elliptischen Kurven brainpoolP256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.Auth

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
		ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		und NIST P-256 ([FIPS186-4])		
8		ECDSA und RSA Signatur Erzeugung mit Softwarezertifikat für TLS ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256) [RFC-8017] (RSASSA-PKCS1-v1_5)	RSA: 2048 and 3072 Bit ECDSA: Schlüssellänge entsprechend der verwendeten elliptischen Kurven brainpoolP256r1 ([RFC5639]) und NIST P-256 ([FIPS186-4])	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.Auth (FCS_CKM.1.1/NK.Zert)
9		ECDSA Signatur Erzeugung mit Unterstützung der gSMC-K und Verifikation für VPN ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)	[TR-03111] ECDSA [RFC-5639] brainpool [FIPS 180-4] (SHA-256)	Schlüssellänge entsprechend der verwendeten elliptischen Kurve brainoolP256r1 ([RFC5639])	[gemSpec_Krypt], Kap. 3.3.1 und 5.5	FCS_COP.1/NK.Auth
10	Schlüsselaushandlung	Diffie-Hellman Schlüsselaushandlung (DH) für VPN (IPsec IKEv2, diffie-hellman group 14)	[HaC] (DH) [RFC-3526] (DH Group) [RFC-7296] (IKEv2) Siehe Abweichungen: [AVA_ACC], Kap. 4	DH: Gruppe 14 2048 Bit Exponentenlänge 2047 Bits	[gemSpec_Krypt], Kap. 3.3.1	FCS_CKM.2/NK.IKE
11		Elliptic Curve Diffie-Hellman Schlüsselaushandlu ng (ECDH) für VPN	[SEC1] (ECDH), [RFC-7296] (IKEv2) [RFC-6954] (ECC curves for IKEv2)	Schlüssellänge entsprechend der verwendeten elliptischen Kurven brainpoolP256r1 ([RFC-6954])	[gemSpec_Krypt], Kap. 3.3.1 und Kap. 5.5	FCS_CKM.2/NK.IKE
12		Diffie-Hellman Schlüsselaushandlung (DH) und Elliptic Curve Diffie-Hellman Schlüsselaushandlung (ECDH) für TLS	[HaC] (DH) [SEC1] (ECDH), [RFC-5246]	DH: Gruppe 14 2048 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
			(TLS v1.2) [RFC-3268] (DHE_RSA) [RFC-4492] (EC-DHE_RSA) [RFC-3526] (DH Gruppe 14) Siehe Abweichungen: [AVA_ACC], Kap. 4	Exponentenlänge = 2048 Bits ECDH: Schlüssellänge entsprechend der verwendeten elliptischen Kurven P-{256,384} ([FIPS186-4]) und brainpoolP{256, 384}r1 ([RFC7027])		
13	Schlüsselableitung	HMAC Berechnung für VPN (PRF) PRF-HMAC-SHA-256	[IANA] mit [RFC-8247#2.2] [FIPS 180-4] (SHA) [RFC-2404] (HMAC) [RFC-7296] (IKEv2)	und 256 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.HMAC
14		Schlüsselableitung für TLS 1.2	[RFC-5246] (TLS v1.2) [FIPS-180-4] (SHA), [RFC-2104] (HMAC),	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_CKM.1/NK.TLS
15	Schlüsselgenerierung	RSA Schlüssel generierung im X.509 und PKCS#12 Format	[RFC4055] (sup. [RFC5280]), [RFC7292] (PKCS#12) [FIPS186-4] (Method B.3.3) Siehe Abweichungen: [AVA_ACC], Kap. 4	3072 Bit	TR 03116-1	FCS_CKM.1/NK.Zert
16		ECC Schlüssel generierung im X.509 Format	[TR-3111] (ECKeyPair) [RFC-5639] (brainpool)	Schlüssellänge entsprechend der verwendeten elliptischen	TR 03116-1	FCS_CKM.1/NK.Zert

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
		Elliptic Kurve Key Pair Generation		Kurve NIST P-256 ([FIPS186-4])		
17	Integrity	HMAC Berechnung und Prüfung für VPN HMAC mit SHA-256	[FIPS 180-4] (SHA) [RFC-2104] (HMAC) [RFC-4868] (HMAC-SHA-2 mit IPsec) [RFC-7296] (IKEv2)	256 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.HMAC
18		HMAC Berechnung und Prüfung für TLS HMAC mit SHA-1, SHA-256 und SHA-384	[FIPS 180-4] (SHA) [RFC-2104] (HMAC) [RFC-5246] (TLS v1.2)	160 Bit, 256 Bit und 384 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.HMAC
19	Vertraulichkeit	Symmetrische Verschlüsselung 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) [RFC-4301] (IPsec)	256 Bit	[gemSpec_Krypt], Kap. 3.3.1	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
20		Symmetrische Verschlüsselung und Entschlüsselung für TLS v1.2 AES-128 und AES-256 in CBC	[FIPS 197] (AES) [RFC-3602] (AES-CBC) [RFC-3268] (AES-TLS mit DH) [RFC-4492] (AES-TLS mit ECDH)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.AES
21	Vertraulichkeit mit Nachrichtenauthentizität (Authenticated Encryption)	AES-128 und AES-256 in GCM Mode für TLS 1.2	[FIPS 197] (AES) [RFC-3268] (AES-TLS) [SP 800-38D] (GCM)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2	FCS_COP.1/NK.TLS.AES

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bit[8]	Anwendungsstandard	Kommentar
			[RFC-5289] (AES-GCM-TLS) [RFC-5116] (AEAD)			
22		Symmetrische Verschlüsselung und Entschlüsselung bei IKE und ESP für VPN Kommunikation AES-GCM-128 und AES-GCM-256 mit 12 und 16 Byte großem ICV	[FIPS 197] (AES) [RFC-4303] (ESP) [RFC-4301] (IPsec) [RFC-4106] (AES-GCM)	AES-GCM: 128 und 256 Bit und 128 Bit Tag Länge	[gemSpec_Krypt], Kap. 3.3.1 und Kap. 5.5	FCS_COP.1/NK.IPsec FCS_COP.1/NK.ESP
23	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
24		VPN IPsec (IKEv2) mit Zertifikatbasierter Authentisierung	[RFC-4301] (IPsec) [RFC-4303] (ESP) [RFC-7296] (IKEv2) [SMD3_NK] [SMD3_MS]	-	[gemSpec_Krypt], Kap. 3.3.1	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS

Tabelle 9: EVG Kryptographische Funktionen

#	Zweck	Kryptographischer Mechanismus	Implementierungsstandard	Schlüssellänge in Bits	Sicherheitsniveau über 120 Bits	Kommentar
1	Authentizität	GPG ECDSA signature verification using brainpoolP384R1 with SHA2-384	[RFC-4880] (OpenPGP) [ANSI X9.62] (ECDSA), BSI TR-03111 ,	384 Bit	yes	Signatureverifikation des Firmware Updates[10] FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update

[10] Hinweis: Dergleiche Mechanismus der Signaturprüfung wird im Rahmen des Secure-Boot Vorgangs (Start der TOE-Bestandteile Netzkonnektor- und Anwendungkonnektor) benutzt.

			[FIPS 180-4] (SHA)			
2		ECDSA signature verification using brainpoolP384R1 with SHA2-384 (UpdateInfo.xml) / brainpoolP256R1 with SHA2-256 (FirmwareGroupInfo.xml)	[ANSI X9.62] (ECDSA), BSI TR-03111 [FIPS 180-4] (SHA)	384 / 256 Bit	yes	Signatureverifikation der UpdateInfo.xml und FirmwareGroupInfo.xml FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update

Tabelle 10**:** EVG Kryptographische Funktionalität (Update und Backup)

Die Stärke der angegebenen kryptografischen Algorithmen war in diesem Zertifizierungsprozess nicht Gegenstand der Untersuchung (siehe BSIG Abschnitt 9, Para. 4, Klausel 2).

Die Evaluatoren haben im Rahmen der Untersuchungen des Source Codes auch die Implementierung der Tabelle 9 und Tabelle 10 aufgeführten Kryptoalgorithmen untersucht. Dabei wurden entweder keine Abweichungen zum jeweiligen Implementierungsstandard festgestellt oder die in den entsprechenden, zusätzlich angegebenen Referenzen beschriebenen Abweichungen auf korrekte Umsetzung geprüft.

4 Ergänzende Angaben zum EVG

4.1 Sicherheitspolitiken des EVG

<Beginn>Erforderliche Übersicht in editierbarer Form

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. Daher setzt der EVG um, dass Sicherheitsfehlfunktionen unterbleiben und schützenswerte Daten nicht abfließen. Weitere Details hierzu können dem Security Target, [ST], Abschnitt 6, entnommen werden.

<Ende>Erforderliche Übersicht in editierbarer Form

4.2 Annahmen und Abgrenzung

<Beginn>Erforderliche Übersicht in editierbarer Form

Die im Security Target definierten Annahmen und einige Aspekte der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht vom EVG alleine abgedeckt. Diese Aspekte führen zu spezifischen Sicherheitszielen, die durch Sicherheitsmaßnahmen der IT-Einsatzumgebung, durch den Nutzer oder durch den Risikomanager erbracht werden müssen. Folgende Aspekte sind im vorliegenden Fall relevant:

Sicherheitsziele der Umgebung wie im Security Target definiert	Kurzbeschreibung anhand des Security Targets	Verweis auf das Benutzerhandbuch
OE.NK.RNG	Externer Zufallszahlengenerator	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.Echtzeituhr	Echtzeituhr	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.Zeitsynchro	Zeitsynchronisation	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.gSMC-K	Sicherheitsmodul gSMC-K	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.KeyStorage	Sicherer Schlüsselspeicher	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.AK	Korrekte Nutzung des EVG durch Anwendungskonnektor	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung

OE.NK.CS	Korrekte Nutzung des Konnektors durch Clientsysteme und andere aktive Komponenten im LAN	[AGD], section 5.4
OE.NK.Admin_EVG	Sichere Administration des Netzkonnektors	[AGD], sections 5.2, 5.3 und 5.4
OE.NK.PKI	Betrieb einer Public-Key-Infrastruktur und Verteilung der TSL	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.phys_Schutz	Physischer Schutz des EVG	[AGD], section 5.1
OE.NK.sichere_TI	Sichere Telematikinfrastruktur-Plattform	Dieses Sicherheitsziel adressiert den Betreiber der TI. Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.kein_DoS	Keine denial-of-service-Angriffe	Dieses Sicherheitsziel adressiert den Betreiber der TI. Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.Betrieb_AK	Sicherer Betrieb des Anwendungskonnektors	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.Betrieb_CS	Sicherer Betrieb der Clientsysteme	[AGD], section 5.4
OE.NK.Ersatzverfahren	Sichere Ersatzverfahren bei Ausfall der Infrastruktur	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.SIS	Sicherer Internet Service	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung
OE.NK.SW-Update	Prozesse für sicheres Software-Update	Keine direkte Aufgabe für den Benutzer zur Einrichtung der Betriebsumgebung

Tabelle 11: Sicherheitsziele der Einsatzumgebung

<Ende>Erforderliche Übersicht in editierbarer Form

4.3 Architekturbeschreibung

<Beginn>Erforderliche Übersicht in editierbarer Form

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

Netzkonnektor:

- VPN-Client
- Dynamischer Paketfilter mit zustandsgesteuerter Filterung
- Netzdienste (Zeitsynchronisation und Zertifikatsprüfung)

- Stateful Packet Inspection
- Selbstschutz (Speicheraufbereitung, Selbsttests, Schutz von Geheimnissen und Seitenkanalresistenz, Sicherheits-Log)
- Administration (Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung und Software Update)
- Kryptographische Basisdienste
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

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

<Ende>Erforderliche Übersicht in editierbarer Form

Part B

Evaluation Results

5 Liste aller ETR-Teile

Die folgenden Einzelprüfberichte (*Single Evaluation Report*) wurden erstellt und mit dem angegebenen Ergebnis (*Result*) bewertet:

Single Evaluation Report	Result
Single Evaluation Report CC Aspect ASE, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.1, 08.09.2025, SRC Security Research & Consulting GmbH, [SER_ASE]	PASS
Single Evaluation Report CC Aspect AGD-ADV, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 3.0, 08.09.2025, SRC Security Research & Consulting GmbH, [SER_AGD_ADV]	PASS
Single Evaluation Report CC Aspect ADV, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.7, 08.09.2025, SRC Security Research & Consulting GmbH, [SER_ADV]	PASS
Single Evaluation Report CC Aspect ALC, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.1, 19.09.2025, SRC Security Research & Consulting GmbH, [SER_ALC]	PASS
Single Evaluation Report CC Assurance Class ATE, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 3.4, 10.02.2026, SRC Security Research & Consulting GmbH, [SER_ATE]	PASS
Single Evaluation Report CC Assurance Class AVA, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9 et al., Version 3.5, 19.11.2025, SRC Security Research & Consulting GmbH, [SER_AVA]	PASS

Die folgende Tabelle beinhaltet eine Zusammenfassung der Ergebnisse (*Result*) einzelner CC Aspekte. Details zu den Ergebnissen finden sich in den referenzierten Einzelprüfberichten.

CC Aspect	Result	Details in
CC Class ASE	PASS	[SER_ASE]
ASE_INT.1	PASS	[SER_ASE]
ASE_CCL.1	PASS	[SER_ASE]
ASE_SPD.1	PASS	[SER_ASE]
ASE_OBJ.2	PASS	[SER_ASE]
ASE_ECD.1	PASS	[SER_ASE]
ASE_REQ.2	PASS	[SER_ASE]
ASE_TSS.1	PASS	[SER_ASE]
ASE_INT.1	PASS	[SER_ASE]
CC Class ALC	PASS	[SER_ALC]
ALC_CMC.3	PASS	[SER_ALC]
ALC_CMS.3	PASS	[SER_ALC]

CC Aspect	Result	Details in
ALC_DEL.1	PASS	[SER_ALC]
ALC_DVS.1	PASS	[SER_ALC]
ALC_LCD.1	PASS	[SER_ALC]
ALC_TAT.1	PASS	[SER_ALC]
ALC_FLR.2	PASS	[SER_ALC]
CC Class ADV	PASS	[SER_AGD_ADV], [SER_ADV]
ADV_FSP.4	PASS	[SER_AGD_ADV]
ADV_TDS.3	PASS	[SER_ADV]
ADV_ARC.1	PASS	[SER_ADV]
ADV_IMP.1	PASS	[SER_ADV]
CC Class AGD	PASS	[SER_AGD_ADV]
AGD_OPE.1	PASS	[SER_AGD_ADV]
AGD_PRE.1	PASS	[SER_AGD_ADV]
CC Class ATE	PASS	[SER_ATE]
ATE_COV.2	PASS	[SER_ATE]
ATE_DPT.1	PASS	[SER_ATE]
ATE_FUN.1	PASS	[SER_ATE]
ATE_IND.2	PASS	[SER_ATE]
CC Class AVA	PASS	[SER_AVA]
AVA_VAN.5	PASS	[SER_AVA]

Part C

Summary

6 Zusätzliche Evaluationsergebnisse

Dieses Kapitel fasst zusätzliche Evaluationsergebnisse zusammen.

6.1 Gültigkeit der Ergebnisse für den RZ Konnektor

Beide Konfigurationen[11] des EVGs secunet konnektor 2.0.0 und 2.1.0 sind binär identisch und unterscheiden sich nur in der Versionierung der HW Komponente (2.0.0 bzw. 2.1.0), genauer um den „HW Version“-Eintrag der FirmwareGruppenInfo (FWGI) bzw. UpdateInfo.

Die Unterschiede der HW sind minimal und haben keinen Einfluss auf die Funktionsweise des EVGs. Insbesondere sind die prozessverarbeitenden Komponenten identisch. Eine detaillierte Analyse aller Unterschiede zwischen EBK und RZK (TOE und non-TOE Anteile) findet sich in [ETR_RZK_1128], Kapitel 6.

Alle Prüfergebnisse in [SER_ASE], [SER_AGD-ADV], [SER_ADV], [SER_ALC], [SER_ATE] und [SER_AVA] gelten für den EVG secunet konnektor 2.0.0 und 2.1.0.

6.2 Zusammenfassung Konnektor-Evaluierung (Evaluierungshinweise)

Das BSI pflegt für die Evaluierung von eHealth Konnektoren eine sogenannte Liste der Evaluierungshinweise ([BSI_Liste]).

Die Prüfstelle bestätigt, dass alle Punkte der Liste im Rahmen der Evaluierung auf Umsetzung geprüft wurden und kommt zu dem Schluss das der EVG den in [BSI_Liste] formulierten verpflichtenden Anforderungen genügt. Alle Punkte wurden mit dem BSI diskutiert und geklärt. Die Analyseergebnisse der Prüfstelle sind im Dokument [BSI_Liste_analysis] dokumentiert.

6.3 Einsatz verschiedener gSMC-Ks

In der Hardware des EVGs werden folgende gSMC-Ks eingesetzt:

- STARCOS 3.6 Health SMCK R1 oder
- TCOS Security Module Card - K Version 2.0 Release 1

verbaut. Je Konnektor werden dabei gSMC-Ks genau eines Herstellers verbaut.

Die Prüfstelle hat den EVG bzgl. des Einsatzes verschiedener gSMC-K bereits im Vorverfahren BSI-DSZ-CC-1135-2020 untersucht und kam zu folgendem Ergebnis:

Beide Karten werden nur mit Kommandos verwendet, die zum Nicht-Optionalen Umfang der Spezifikationen für die gSMC-K bzw. das unterliegende COS gehören. Insbesondere wird nur der in [gemSpec_COS] spezifizierte Funktionsumfang verwendet und keine darüberhinausgehenden herstellerspezifischen Kommandovarianten. Mögliche Optionen und Funktionsvarianten der der G2 COS-Spezifikation oder der Objektsystem-Spezifikation spielen für die Nutzung durch Secunet keine Rolle. Daher gibt es keine Unterschiede bei der Benutzung beider Karten.

[11] Siehe [ST], Kap. 1.2.1.

Zudem wird im Konnektor dieselbe Software für beide Karten verwendet. Daher verhalten sich beide Karten im Konnektor gleich.

Die jeweiligen TR-Konformitätsreports zu BSI-K-TR-0227-2016 und BSI-K-TR-0226-2015 führen jeweils in Kapitel 9.1 Auflagen und Hinweise für den Einsatz, die Herstellung & Auslieferung des Prüfgegenstands auf. Es gibt darin keine Auflagen und Hinweise an den Einsatz der gSMC-K, die zu einem unterschiedlichen Verhalten der gSMC-Ks bei der Verwendung durch den secunet konnektor 2.0.0 und 2.1.0 führen.

Der Hersteller hat alle automatisierten Tests für beide Kartentypen durchgeführt. SRC hat als Stichprobe die Funktion der GUI entsprechend [AGD], Kapitel 9.3.1 aufgerufen, mit deren Hilfe man die Karten identifizieren kann und dies für Kartentypen geprüft. Dies wurde für den aktuellen TOE als Beispielfall für den Kartentyp STARCOS (Wert 1) sowie TCOS (Wert 0) durchgeführt:

Seriennummer des EVG	ICCSN	11. Ziffer (Kartenhersteller)
306/20/36-0100009	80276883660000002853	0 (STARCOS)
306/20/36-0100016	80276883661000000143	1 (T-SYSTEMS)

Tabelle 12: Identifikation der gSMC-Ks am Konnektor.

Ergänzung für PTV5:

In der Hardware des EVGs werden zusätzlich folgende gSMC-Ks eingesetzt:

- STARCOS 3.6 Health SMCK R1 (mit ECC Unterstützung)
- STARCOS 3.7 gSMC-K R1 oder
- TCOS Security Module Card - K Version 2.0 Release 2

Die neu hinzugekommenen Karten sind vom gleichen Typ und Hersteller, wie die bereits in Verwendung befindlichen gSMC-Ks. Die jeweiligen TR-Konformitätsreports zu BSI-K-TR-0408-2021 und **BSI-K-TR-0469-2021** führen jeweils in Kapitel 9.1 Auflagen und Hinweise für den Einsatz, die Herstellung & Auslieferung des Prüfgegenstands auf. Es gibt darin keine Auflagen und Hinweise an den Einsatz der gSMC-K, die zu einem unterschiedlichen Verhalten der gSMC-Ks bei der Verwendung durch den secunet konnektor 2.0.0 und 2.1.0 führen. Der Hersteller führt hierzu eigene Kompatibilitätstests im Rahmen der Entwicklung durch. Die Identifikation dieser gSMC-K kann ebenfalls wie in [AGD], Kapitel 9.3.1 beschrieben erfolgen.

6.4 Wiederverwendung von Auditergebnissen

Ergänzung für PTV4:

Im Rahmen der vorangegangenen Evaluierung zu PTV4 BSI-DSZ-CC-1044-V4 wurde für den Standort #4 aus Tabelle 8 eine geringfügige Änderung der Prozesse im Kontext des Konfigurationsmanagements umgesetzt. Hierbei wurde ein manueller Prozessschritt durch ein automatisiertes Skript ersetzt. Die Änderung wurde seitens des Herstellers maßgeblich in den Do-

kumenten [SecEnvChange] und [CodeImport_eHx] notiert. Die Änderung hat keine Auswirkung auf das Verdikt von [SER_ALC] und insbesondere auf die vorhandenen Ergebnisse der entsprechenden Begehung.

Ergänzung für PTV5:

Bezogen auf die letzte EVG Aktualisierung erfolgte im Bereitstellungsprozess eine geringfügige Anpassung eines internen Prozesses an der Schnittstelle der Standorte #1 und #4 aus Tabelle 8. Hierbei wurde das Format des in einem internen Lieferungsprozess ausgetauschten Artefakts, welches die Implementierung des Anwendungskonnektors enthält, verändert. Der Hersteller hat die Beschreibungen in der internen Dokumentation entsprechend angepasst, [ExchangeChange]. Diese Änderung hat keine Auswirkung auf die Sicherheit des EVGs, da die Integrität des Artefakts weiterhin durch eine kryptographische Signatur sichergestellt wird.

Die Änderung hat keine Auswirkung auf das Verdikt von [SER_ALC] und insbesondere auf die vorhandenen Ergebnisse der entsprechenden Begehung.

Des Weiteren wurden die produktspezifischen Aspekte ALC_CMS und ALC_TAT im Rahmen der Evaluierung für den vorliegenden EVG neu betrachtet.

Ergänzung für PTV5 WR1:

Keine Änderungen gegenüber dem Basisverfahren PTV5.

Es wurden nur die produktspezifischen Aspekte ALC_CMS und ALC_TAT im Rahmen der Evaluierung für den vorliegenden EVG neu betrachtet.

Ergänzung für PTV5 Plus (WR3):

Im Rahmen des Verfahrens wurden alle Standorte erneut auditiert und die Sicherheit der Umgebung bestätigt, siehe Kapitel 3.3.

Ergänzung für PTV5 Plus (WR4):

Keine Änderungen gegenüber dem Basisverfahren PTV5 Plus (WR3, inkl. ALC Re-Evaluierung BSI-DSZ-CC-1044-V7-2023-MA-02). Die Auditergebnisse wurdem gemäß der Absprache mit der Zertifizierungsstelle, [KickOff-1209-V2] und im Einklang mit [JIL_CrisisPol] wiederverwendet.

Es wurden nur die produktspezifischen Aspekte ALC_CMS und ALC_TAT im Rahmen der Evaluierung für den vorliegenden EVG neu betrachtet.

Ergänzung für PTV6:

Im Rahmen des Verfahrens wurden alle relevanten Standorte erneut auditiert und die Sicherheit der Umgebung bestätigt, siehe Kapitel 3.3.

6.5 Zusätzliche Evaluationsergebnisse zum Laufzeitverlängerung in PTV5 Plus (WR3)

Die Änderung am ST in Bezug auf das Feature „Laufzeitverlängerung“ betrifft ein neues Objekt O_LZV_Zert_gSMCK**,** welches die gemäß TUC_KON_410 in [gemSpec_Kon] zu aktualisierenden Zertifikate aufnimmt. Dieses Objekt wird durch die SFR FDP_ITC.2.5/NK.TLS sowie FMT_MTD.1.1/**AK.**Admin aufgegriffen, um die Import-Funktionalität und die Zugriffsberechtigung des Administrators für diese Funktionalität im TOE zu modellieren. Das Kapitel 8.5 im [ST] beschreibt die entsprechende Funktionalität anhand von Referenzen zur [gemSpec_Kon], A_21736 / A_21744 / TUC_KON_410.

Die oben genannten Änderungen erfolgten zeitlich spät in der Evaluierung, weswegen hier gesondert der Einfluss auf die Evaluationsberichte [SER_ASE], [SER_AGD-ADV], [SER_ADV] und [SER_ATE] nach deren Fertigstellung zusammenfassend eingegagnen wird. Die genannten Berichte wurden an die genannten Änderungen angepasst. Der Evaluator stellte fest, dass die von der Laufzeitverlängerung nicht betroffenen Ergebnisse in den Berichten weiterhin gültig sind.

Im Rahmen der Evaluierung zum Aspekt ADV_IMP wurde die Implementierung der Funktionalität zur Laufzeitverlängerung untersucht und die Ergebnisse maßgeblich in [SER_ADV], Table 8 ausgeführt. Dies betrifft insbesondere den Import und die Validierung der erneuerten Zertifikate, bevor diese im EVG zum Einsatz kommen.

Im Rahmen der Evaluierung zum Aspekt ATE_FUN hat der Evaluator eine Analyse der Herstellertests in Bezug auf die Laufzeitverlängerung durchgeführt und das Ergebnis im [SER_ATE], Table 23 dokumentiert.

Des Weiteren wurden die gemäß [BSI_Liste_LZV] speziell zu berücksichtigenden Aspekte analysiert und die entsprechenden Ergebnisse und Informationen rund um die Laufzeitverlängerung im TOE in [BSI_Liste_LZV_Analyse] für das BSI dargelegt.

Das Feature „Laufzeitverlängerung“ wurde im Rahmen der Schwachstellenanalyse in [SER_AVA] berücksichtigt, wobei die Analyse zeigte, dass damit keine neuen Angriffsvektoren hinzugekommen sind bzw. die bestehenden Sicherheitsmaßnahmen diese abdecken und bereits evaluiert sind.

6.6 Gültigkeit der Evaluationsergebnisse für die EVG Version 6.0.8 in PTV6

Im Rahmen der Feldnutzung und von Tests wurden seitens des Herstellers noch während der Evaluierung einige Fehler festgestellt, welche durch die aktuelle Version 6.0.8 des EVGs behoben werden. Der Hersteller hat diese Version (Source-Code und EVG-Images), inklusive der Änderungsbeschreibungen in [CHANGES], sowie zusätzliche Testergebnisse in [ATE_REPORT] und spezifische Testergebnisse in [ATE_IAR_6.0.8] und [ATE_IAR_6.0.13] bereitgestellt. Auf Basis der vorgelegten Änderungsbeschreibungen konnte festgestellt werden, dass die Änderungen funktional sind und die Sicherheitsfunktionalität gemäß der Sicherheitsvorgaben nicht beeinflussen. Die korrekte Funktionalität nach Änderungen wurde vom Hersteller durch die bereitgestellten Testergebnisse nachgewiesen und anhand dieser vom Evaluator verifiziert. Die meisten der Evaluationsergebnisse wurden im Rahmen der Evaluierung auf der Vorversion 6.0.5 des EVGs erzielt. Der Evaluator kam auf der Basis der oben genannten Untersuchung zu dem Schluss, dass diese Ergebnisse, insbesondere betreffend

der [SER_ASE], [SER_AGD-ADV], [SER_ADV], [SER_ATE] und [SER_AVA] inklusive der Unteraspekte (siehe auch Kap. 3.2), auf die finale EVG Version 6.0.8 übertragbar sind.

7 Fehler und Inkonsistenzen

Dieses Kapitel fasst Fehler und Inkonsistenzen, die im Rahmen der Evaluierung für den finalen EVG ermittelt wurden, zusammen.

Die Evaluatoren haben keine Fehler und Inkonsistenzen im Rahmen der Evaluierung festgestellt, die den finalen EVG betreffen.

8 Schwachstellen

Dieses Kapitel fasst die Schwachstellen die im Rahmen der Evaluierung für den finalen EVG ermittelt wurden zusammen.

Die Evaluatoren haben keine Schwachstellen im Rahmen der Evaluierung festgestellt, die den finalen EVG betreffen.

9 Auflagen und Hinweise

Dieses Kapitel fasst zusätzliche Auflagen und Hinweise aus den Kapiteln "questions, recommendations to the developer" und "necessary changes" der Einzelprüfberichte zusammen.

9.1 Auflagen und Hinweise an den Hersteller

Die Evaluatoren haben keine Auflagen und Hinweise an den Hersteller im Rahmen der Evaluierung festgestellt, die den finalen EVG betreffen.

9.2 Auflagen für den Einsatz des evaluierten Produkts

Deutsche Fassung

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

- Die EVG Konfiguration sieht eine verpflichtende Nutzung von TLS sowie eine verpflichtende Client-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 “inReihe”, da diese eine höhere Sicherheit der angeschlossenen LAN-seitigen Netzwerke bietet, siehe [AGD], Kapitel 10.2.1.2.

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

Englische Fassung

The TOE is only able to provide its security services under the following conditions:

- The TOE is configured with mandatory TLS and mandatory client authentication.
- The connected client systems verify the authenticity of the Konnektor when using services and receiving events.
- The user is able to identify whether a client system connection is secure.

The TOE user shall only operate the TOE under the conditions above. A violation of these conditions is considered a vulnerability of the TOE in the operational environment. In this case, the TOE user is responsible to counter the vulnerability.

The TOE supports different setups. The main setups are “Parallel” Mode, “InReihe” Mode and Offline Mode. The “InReihe” Mode is recommended since it provides a higher protection of the connected LAN, refer to section 10.2.1.2 of [AGD].

For the active VPN connections using IPsec no countermeasures against statistic traffic analysis are implemented.

10 Re-Evaluierung und Wiederverwendung

Alle Subsysteme sind bei der Umsetzung der TSF beteiligt. Sofern ein Subsystem verändert wird, muss der Einfluss der Änderung auf die Sicherheit des Produktes analysiert und bewertet werden. Wenn nötig, muss ein Re-Zertifizierungsprozess initiiert werden.

11 Abschließendes Votum der Prüfstelle

Sofern im Verlauf der Evaluierung Erkenntnisse gewonnen wurden, die Auswirkungen auf die Aussagen schon fertiggestellter ETR-Teile hatten, wurden diese Erkenntnisse in überarbeiteten Fassungen der betroffenen ETR-Teile berücksichtigt bzw. in Kapitel 6 dokumentiert. Es wurde von den Evaluatoren abschließend geprüft, dass die Aussagen aller unter Kapitel 5 und 6 aufgeführten ETR-Teile bzw. Ergänzungen zutreffend sind.

Die Liste aller erkannten Fehler und Inkonsistenzen in Kapitel 7, die Liste aller verbleibenden (residualen) Schwachstellen in Kapitel 8 und die Auflagen und Hinweise in Kapitel 9 sind eine vollständige Zusammenfassung der entsprechenden Ergebnisse aller in Kapitel 5 und 6 dargelegten Prüfergebnisse.

Die in Kapitel 10 festgehaltene Klassifikation der Subsysteme und Module des EVGs in sicherheitsspezifisch / sicherheitsrelevant bzw. SFR-enforcing / SFR-supporting ist aus abschließender Sicht zutreffend.

Auf der Grundlage der in den ETR-Teilen dokumentierten Evaluierungsergebnisse kommen die Evaluatoren zu folgendem Prüfergebnis:

1. Der EVG ist konform zum PP
    - Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.7, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)
2. Die Konformität des EVG zum PP ist: strikt („strict conformance“)
3. Die Sicherheitsfunktionalität ist
    - PP konform, und
    - um produktspezifische Aspekte ergänzt, und
    - Common Criteria Teil 2 erweitert
4. Die verwendeten Vertrauenswürdigkeitskomponenten
    - sind Common Criteria Teil 3 konform, und
    - sind PP-konform, und
    - die Anforderungen der Stufe **EAL3 augmentiert um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5** und **ALC_FLR.2**, sind erfüllt.
5. Alle in den Sicherheitsvorgaben geäußerten Sicherheitsziele für den EVG werden erreicht.
6. Die in den Sicherheitsvorgaben geäußerten funktionalen Sicherheitsanforderungen für den EVG werden erreicht.
7. Der EVG widersteht dem Angriffspotential: **High**

Beteiligtes Personal

Evaluator(en)	Siehe Auflistung in Kapitel 1.3, Tabelle 4 auf Seite 11.
Alle an dieser Evaluierung beteiligten Personen sind in der wahrgenommenen Rolle angeführt. Die Unabhängigkeit und Unparteilichkeit der Evaluatoren war gewährleistet und sie hatten die für die Prüfung notwendigen Mittel / Ressourcen zur Verfügung. Die Prüfberichte geben die tatsächlichen Fakten und Ergebnisse wieder und sind durch keine anderen Sachverhalte als die zwischen Prüf- und Zertifizierungsstelle bestehenden beeinflusst	
Projektleiter der Evaluierung	Mark Schall
Unterschrift Projektleiter der Evaluierung	
Das Verfahren ist gemäß den im Rahmen der Anerkennung durch das BSI abgenommenen Prozessen der Prüfstelle durchgeführt und eventuelle Abweichungen sind individuell dokumentiert und werden von der Prüfstellenleitung verantwortet. Formale und inhaltliche QS wurde wie auf den Dokumenten vermerkt durchgeführt.	
QMB:	David Seim
Unterschrift QMB:	

A. Bibliografie

A.1. Evaluation Documents

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[NK-PP] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.7, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AK-PP] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Version 1.6.1 vom 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[PPCOS] Common Criteria Protection Profile: Card Operating System (PP COS G2), BSI-CC-PP-0082-V4, Version 2.1 vom 10.07.2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[gemSpec_COS] Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[gemProdT_Kon_PTV5] Produkttypsteckbrief Prüfvorschrift Konnektor gemProdT_Kon_PTV6_6.0.2-0_V1.0.0

[gemSpec_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec_Kon], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 5.25.0, 03.04.2025

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.40.0, 28.03.2025

[gemSpec_Net] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 1.23.0, 16.12.2022

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

[AIS14] Anwendungshinweise und Interpretationen zum Schema, AIS 14: Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) Version 7, 03.08.2010

[AIS19] Anwendungshinweise und Interpretationen zum Schema, AIS 19: Anforderungen an Aufbau und Inhat der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, 03.11.2014

[AIS20] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[AIS32] Anwendungshinweise und Interpretationen zum Schema, AIS 32, Interpretationen und Korrekturen zur CC, Version 7, 08.06.2011

[AIS34] Anwendungshinweise und Interpretationen zum Schema, AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 03.09.2009

[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

[SOGIS-ACM] SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, version 1.3, 2023

A.2. Legislatives and Standards

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

[HMAC_SHA1] C. Madson, R. Glenn: Use of HMAC-SHA-1-96 within ESP and AH, November 1998, RFC 2404, http://www.rfc-editor.org/rfc/rfc2404.txt

[HMAC_SHA2] S. Kelly, S. Frankel: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. May 2007, RFC 4868, http://www.rfc-editor.org/rfc/rfc4868.txt

[RFC5996] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen: Internet Key Exchange (IKEv2) Protocol, September 2010, RFC 5996 (IKEv2), http://www.ietf.org/rfc/rfc5996.txt

[RCF3447] J. Jonsson, B. Kaliski: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. February 2003. RFC 3447, http://www.rfc-editor.org/rfc/rfc3447.txt[RFC2131] Dynamic Host Configuration Protocol; R. Droms; March 1997. RFC 2131, https://tools.ietf.org/html/rfc2131

[RFC3602] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003, RFC 3602, http://www.rfc-editor.org/rfc/rfc3602.txt

[RFC4303] S. Kent: IP Encapsulating Security Payload (ESP), December 2005, RFC 4303 (ESP), http://www.ietf.org/rfc/rfc4303.txt

[RFC4301] S. Kent, K. Seo: Security Architecture for the Internet Protocol, December 2005, RFC 4301 (IPsec), http://www.ietf.org/rfc/rfc4301.txt

[RFC3526] T. Kivinen, M.Kojo: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). May 2003, RFC 3526, http://www.rfc-editor.org/rfc/rfc3526.txt

[RFC4346] RFC 4346 T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006

[RFC5246] RFC 5246 T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008

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

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

[RCF4492] Blake-Wilson, et al., Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), RFC 4492, May 2006

[RFC5289] E. Rescorla, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), RFC 5289, August 2008

[RFC4055] J. Schaad, B. Kaliski, R. Housley: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. June 2005, RFC 4055, https://www.rfc-editor.org/rfc/rfc4055.txt

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (May 2008), https://www.ietf.org/rfc/rfc5280.txt

[PKCS12] PKCS #12 v1.0: Personal Information Exchange Syntax. June 1999, RSA Laboratories

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

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

[RFC2404] C. Madson, R. Glenn: Use of HMAC-SHA-1-96 within ESP and AH, November 1998, RFC 2404, https://www.rfc-editor.org/rfc/rfc2404.txt

[RFC4868] S. Kelly, S. Frankel: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. May 2007, RFC 4868, https://www.rfc-editor.org/rfc/rfc4868.txt

[RFC7296] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, RFC 7296 (IKEv2), https://www.ietf.org/rfc/rfc7296.txt

[FIPS197], [AES] NIST FIPS 197: Advanced Encryption Standard (AES). November 2001

[RFC8017] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch: PKCS #1: RSA Cryptography Specifications Version 2.2. November 2016. RFC 8017, https://www.rfc-editor.org/rfc/rfc8017.txt

[RFC5116] An Interface and Algorithms for Authenticated Encryption, D. McGrew, January 2008

[RFC7027] J. Merkle, M. Lochter, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), October 2013, https://www.rfc-editor.org/rfc/rfc7027.txt

[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, OpenPGP Message Format, November 2007, https://www.rfc-editor.org/rfc/rfc4880.txt

[CAdES] ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

[CAdES_BP] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); CAdES Baseline Profile; ETSI Technical Specification TS 103 173, Version 2.1.1, 2012-03

[PAdES] ETSI TS 102 778-3 V1.2.1, PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles Technical Specification, 2010

[PAdES_BP] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); PAdES Baseline Profile; ETSI Technical Specification TS 103 172, Version 2.1.1, 2012-03

[XMLSig] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[XMLEnc] XML Encryption Syntax and Processing, Version 1.1 W3C Recommendation, 11 April 2013, https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/

[XAdES] XML Advanced Electronic Signatures (XAdES), European Telecommunications Standards Institute (ETSI): Technical Specication XML Advanced Electronic Signatures (XAdES). ETSI Technical Specication TS 101 903, Version 1.4.2, 2010

[XAdES_BP] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); XAdES Baseline Profile; ETSI Technical Specification TS 103 171, Version 2.1.1, 2012-03

[RFC3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, W. Polk, R. Housley, L. Bassham, April 2002

[RFC5639] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, J. Merkle, March 2010

[RFC5652] RFC 5652 (September 2009): Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc5652.txt

[RFC5751] RFC 5751 (Januar 2010): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, Message Specification, http://www.ietf.org/rfc/rfc5751.txt (für MIME s. RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049)

[RFC5083] Housley: Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, RFC 5083, November 2007, https://tools.ietf.org/html/rfc5083

[RFC5084] R. Housley: Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), RFC 5084, November 2007, https://tools.ietf.org/html/rfc5084

[ISO 9796-2] ISO 9796-2: 2002, Information technology – Security techniques – Digital signature schemes giving Message Recovery – Part 2: Mechanisms using a hash function Update

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

[SEC1] Standards for Efficient CryptographySEC 1: Elliptic Curve CryptographyCerticom ResearchContact: Daniel R. L. Brown (dbrown@certicom.com)May 21, 2009Version 2.0

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

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

[TR-02102-3] Technische Richtlinie TR-02102-3 Kryptographische Verfahren:Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2023-01

[TR-03111] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.10, 01.06.018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

A.3. Developer Documents

A.3.1. Security Target (ASE)

[ST] BSI-DSZ-CC-1209-V3:
Security Target für secunet konnektor 2.0.0 und secunet konnektor 2.1.0, Version 1.32, 05.02.2026, secunet Security Networks AG
file name: 1209-v3_ST secunet konnektor v1.32_05022026.pdf

BSI-DSZ-CC-1044-V9
Security Target für secunet konnektor 2.0.0 und secunet konnektor 2.1.0, Version 3.3, 05.02.2026, secunet Security Networks AG

file name: 1044-v9_ST_secunet_Netzkonnektor_v33_changes_05022026.pdf

A.3.2. **Functional specification (ADV_FSP)**

[FSP] Funktionale Spezifikation secunet konnektor 2.0.0, 2.0.1 und 2.1.0, Version v5.2, 28.03.2025
file name: FSP_secunet_eHealth konnektor_v52_PTV6_250328.pdf

[FSP_LED] Funktionale Spezifikation, LED-Beschreibung, Version 1.9.6, 21.03.203, file name: secunet-konnektor_LED-Konzept.pdf

[REST-API] Konnektor Management API-Dokumentation, eHealthExperts, Version 6.0.1**,** Stand 20.08.2025
file name: Modularer_Konnektor_API_Dokumentation_6.0.5.pdf

[FM-API] Fachmodulschnittstelle des Basiskonnektors 6.0.4 API, eHealthExperts; Version 1.11, 23.06.2025,
file name: Fachmodulschnittstellen-javadoc-1.11.zip

[FSP_AK_COS_KT] Funktionale Spezifikation COS und KT, Schnittstellen zu den Karten des Gesundheitswesens und SICCT Kartenterminals, Version: 1.0.0, Datum: 19.06.2020, file name: FSP_AK_COS_KT_v1.1

[gSMC-K] Konformitätsreport, BSI-K-TR-0227-2016, STARCOS 3.6 Health SMCK R1, Giesecke & Devrient GmbH

Konformitätsreport, BSI-K-TR-0226-2015, TCOS Security Module Card - K Version 2.0 Release 1, T-Systems International GmbH

Konformitätsreport, BSI-K-TR-0408-2021, STARCOS 3.7 gSMC-K R1, Giesecke+Devrient Mobile Security GmbH

Konformitätsreport, BSI-K-TR-0469-2021, TCOS Security Module Card – K Version 2.0 Release 2, Deutsche Telekom Security GmbH

A.3.3. **Guidance (AGD)**

[AGD] secunet(konnektor, Bedienungsanleitung, Für Administratoren und Benutzer, Version 7.4, 23.10.2025, Secunet Security Networks AG

Inklusive [AGD_Errata]: -

[AGD_DEL] secunet(konnektor v2.0.0, 2.0.1 und 2.1.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, secunet Security Networks AG, Version 2.0, 11.05.2023

[FM-SEC] Security Guidance Fachmodulentwicklung; eHealthExperts; v2.0; 25.06.2025;
file name: security-guidance-fachmodulentwicklung 2.0.pdf

A.3.4. **Security architecture (ADV_ARC)**

[ARC_NK]	secunet(konnektor Version 2.0.0 und 2.1.0, Sicherheitsarchitektur, Version 2.8, 29.08.2025
[ARC_AK]	eHealthExperts EHX Group, Security Architecture (ADV_ARC), Anwendungskonnektor, Version 2.8, 14.10.2025
[SMT1]	SINA Workstation S, E, H and SINA Box S, Crypto File System (CFS), secunet Security Networks AG, Version: 1.5, 3.11.2016
[SMT5]	secunet konnektor Version 2.0.0 und 2.1.0, VirtualBox, Version 1.1, 21.06.2021, secunet Security Networks AG
[SMT6], [SMT6a]	Documentation and Analysis of the Linux Random NumberGenerator, Version 3.6, 2020-04-07, atsec information security GmbH Including: Übersicht über Linux-Kernel mit NTG.1-oder DRG.3-konformem Zufallszahlengenerator /dev/random, Stand: Juli 2020, Bundesamt für Sicherheit in der Informationstechnik
[Rand_Server]	secunet konnektor Version 2.0.0 und 2.1.0, Rand Server, Version 1.2, 16.11.2020 Including: [Zufall] secunet konnektor Version 2.0.0 und 2.1.0, Konzept Zufallszahlen, Version 2.4, 24.05.2022
[Dev_RNG]	NIST SP 800-90A Deterministic Random Bit Generator (DRBG) im EBK/RZK, Implementationsdetails; 06.01.2025; Version: 1.2; document name: NIST-SP-800-90A-DRBG-Connector_v1.2.pfd.
[SMT9]	secunet(konnektor Modularer Konnektor Version 2.0.0 und 2.1.0, Software-Update,Version 2.2.1, 14.08.2025, secunet Security Networks AG
[SMT10]	Modularer Konnektor 2.0.0 und 2.1.0, Kernel-Konfigurationsvergleich 3.18.113/5.4.x, Version 1.1, 14.12.2020 Vergleich der Kernel-Konfigurationen 3.18.x versus 5.4.x als Excel-Sheet (Dateiname: PTV4_ARC_KernelKonfig_210112_v32.xlsx)
[SMT11]	secunet konnektor Version 2.0.0 und 2.1.0, grsecurity, Version 1.0, 03.09.2020, file name: grsecurity_konnektor_v1.0.pdf secunet konnektor Version 2.0.0 und 2.1.0, PAX, Version 1.0, 03.09.2020, file name: PaX_konnektor_v1.0.pdf secunet konnektor Version 2.0.0 und 2.1.0, References grsecurity/PAX, v1.0, 03.09.2020, file name: References_grsecurity_PAX_konnektor_v1.0

[Selbsttest] Modularer Konnektor Version 2.0.0 und 2.1.0, Selbsttest, Version 2.6 vom 20.02.2020

[SME1] see [SME1_1] and [SME1_2]

[SME1_1] secunet Konnektor (CSAS Mainboard): Härtungsmaßnahmen und sicherer Start-up der Firmware, Vsersion: 1.0, Datum: 12.04.2018

[SME1_2] secunet Konnektor (CSAS Mainboard): Härtungsmaßnahmen und sicherer Start-up der Firmware –Zusatzinformationen für BIOS R006 und R007, Version: 0.3, Datum: 23.11.18

[SME1_3] secunet konnektor Version 2.0.0 und 2.1.0, BIOS R011, Version 1.1, 10.03.2020

[SMD1] Geschäftsbereich Hochsicherheit, Richtlinien für die Softwareentwicklung, Version: 1.4, 26.4.2011

[SMD2] CVE Analyse für den secunet Konnektor, Filename: CVE-BSI-Report-2025-05-30-NK-6.0.1.xlsx

[SMD3_AK] RFC-Analyse AK-TLS, Anwendungskonnektor, Version 1.3, 01.07.2025

[SMD3_MS_AK] Nachweis TLS Security, Version 1.1, 15.05.2025, TLSv12_MAY+SHOULD_v1.1.xlsx

[SMD3_NK] Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, Version 0.4, 25.06.2025

[SMD3_MS] IPsec-RFCs - MAY_SHOULD Anforderungen, secunet(konnektor, Version 0.3, 25.06.2025

[SMD4] Herstellerpentestdokumentation:

1. Durchlauf:
   - Prüfkonzept, IT-Sicherheitsanalyse des Konnektors PTV4, Version 0.4, 12.07.2021, eHealth Experts GmbH
   - Testdurchführung, siehe 2. Durchlauf.
   - Ergebnisdokumentation, IT-Sicherheitsanalyse des Konnektors PTV5, Version 0.6, 01.09.2021, eHealth Experts GmbH, inklusive Rohdaten und Logs, 07.09.2021
   - Übersicht Umsetzung Pentestfindings PTV5, Version 1.1 vom 24.09.2021
2. Durchlauf
   - Prüfkonzept, IT-Sicherheitsanalyse des Konnektors PTV5, Version 0.6, 19.10.2021, eHealth Experts GmbH

- Testdurchführung, IT-Sicherheitsanalyse des Konnektors PTV5, Version: 0.5, Datum: 28.10.2021
- Ergebnisdokumentation, IT-Sicherheitsanalyse des Konnektors PTV5, Version 0.8, 28.10.2021, eHealth Experts GmbH, inklusive Rohdaten und Logs, 25.10.2021
- Übersicht Umsetzung Pentestfindings PTV5, Version 1.3 vom 04.11.2021
- Zusatz-Untersuchung: IT-Sicherheitsanalyse Firewall-Regelwerk (PTV5), Version 0.4, 26.11.2021

3. Durchlauf:

- Prüfkonzept, IT-Sicherheitsanalyse des Konnektors PTV5, Version 1.0, 20.12.2021, eHealth Experts GmbH
- Testdurchführung, IT-Sicherheitsanalyse des Konnektors PTV5, Version: 1.0, 20.12.2021
- Ergebnisdokumentation, IT-Sicherheitsanalyse des Konnektors PTV5, Version 1.0, 20.12.2021, eHealth Experts GmbH, inklusive Rohdaten und Logs, 20.12.2021
- Übersicht Umsetzung Pentestfindings PTV5, Version 1.4 vom 18.01.2021

[SMD5] secunet(konnektor Version 2.0.0 und 2.1.0, Static source code analysis, Version 1.3, 15.05.2025, secunet Security Networks AG filename: Static_source_code_analysis_NK_v1.3.pdf, incl. Log-archive: 14052025.zip

Including the ticket EHEX-6339 as stated in PRUEFEBK-11_20250113.doc.

[CVE_Spring] CVE-Analyse Spring-FW, Version V1.1, 27.05.2020, filename: CVE-Analyse Spring-FW_v1.1.xlsx

[CVE_AK] CVE-Analyse, Version 8.2, 17.11.2025, filename: CVE_Analyse_v8.2.xlsx

[CVE-Details] https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&seach_type=all&query=cpe:2.3:o:linux:linux_kernel:5.4.17:*:*:*:*:*:*:*, https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&seach_type=all&query=cpe:2.3:a:oracle:vm_virtualbox:6.1.16:*:*:*:*:*:*:*

[NVD] https://nvd.nist.gov/vuln

[KernelCVEs] https://github.com/nluedtke/linux_kernel_cves/blob/master/data/5.4/5.4

_security.txt,
https://github.com/nluedtke/linux_kernel_cves/blob/master/data/5.4/5.4_CVEs.txt

[NetzInst] secunet(konnektor Version 2.0, Konzept Netzwerkinstallation, Version 0.24, 14.05.2018

A.3.5. **TOE Design (ADV_TDS)**

[TDS] [TDS_NK], [TDS_AK] und [TDS_AK_PTV5]

[TDS_NK] secunet(konnektor Version 2.0.0, 2.0.1 und 2.1.0, Technical Design Specification (ADV_TDS), secunet Security Networks AG, Version 2.25, 04.03.2025
file name: TDS_NK_v2_25_04032025.pdf

[TDS_AK] TOE-Design, Anwendungskonnektor, eHealthExperts GmbH, Version 2.12, 26.06.2025
file name: ADV_TDS_AK_v2.12.pdf

[AK_javadoc] Javadoc 17.06.2025 zu [TDS_AK]:
\connector-app
\connector-basic
\connector-fm-amts
\connector-fm-nfdm
\connector-fm-vsdm

[TDS_AK_PTV5[12]] secunet(konnektor Version 2.0.0 und 2.1.0, Technical Design Specification (ADV_TDS), Subsystem Anwendungskonnektor PTV5-WR1; secunet Security Networks AG, Version 2.0, 28.03.2025
file name: TDS_AK_PTV6_v2_20250328.pdf

[AK_NK] Modularer Konnektor, Entwickler-Dokumentation, Schnittstellenspezifikation, AK/NK, Für die SW-Entwickler eHealthExperts / secunet, Version 4.2 vom 15.08.2024

[SigDir] secunet konnektor Version 2.0.0 und 2.1.0, Signaturdirektive, Version 1.60, 17.09.2024

[EncDir] secunet konnektor Version 2.0.0 und 2.1.0, Verschlüsselungsdirektive, Version 2.0, 21.06.2022

[DokSich] secunet konnektor Version 2.0.0 und 2.1.0, Dokumentensicherheit, Version 1.21, 17.05.2022

12 Document reference kept for consistency in the SERs

Including: Vulnerability Report, Attacks bypassing the signature validation in PDF, November 08, 2018, file name: VulnRepPDFSig.pdf

[WerksR] Modularer Konnektor 2.0.0 und 2.1.0, Spezifikation Werksreset, eHealthExperts GmbH & secunet Security Networks AG, Version 1.8 vom 29.10.2019

[KON_RMK] KON_RMK, Konzept Remote-Management des Konnektors, eHealthExperts GmbH & secunet Security Networks AG, Version 1.0, 28.06.2018

[KON_ALT_TLS] Konzept Alternative TLS Server Authentisierung; eHealthExperts GmbH; Version 1.0, 25.11.2020

[secIP] secunet(konnector Version 2.0.0 und 2.1.0, IP-Stack, Version 1.3, 25.11.2020

[FW_XML] connector-refxman XML configuration, connector-refxman.xml as part of the implementation representation

[strongSwan] https://www.strongswan.org

[StrongSwanConf] https://wiki.strongswan.org/projects/strongswan/wiki/Swanctlconf

[openSSL] https://www.openssl.org/

[mosquitto] http://mosquitto.org/

[bind] https://www.isc.org/downloads/bind/

A.3.6. **Implementation Representation (ADV_IMP)**

[SECU-IMPM] secunet(konnektor, Produktversion 2.0.0 und 2.1.0, Implementation Representation, Version 2.5, 16.10.2025; filename: ADV_IMP_NK_v2.5_2025-10-16.pdf.

[IMP-Krypto] secunet konnektor, Version 2.0.0 und 2.1.0, Kryptographische Mechanismen, Mapping auf die Implementierung, Version 5.1.1, 14.08.2025

[SECU-IMP-NK] Release vom 29.01.2026:

- secunet konnektor 2.0.0 und 2.1.0 im Archiv:
  - Name: konnektor-6.0.8-sourcecode-release.tar.bz2
  - SHA256: 56e06bcc7fea293db1361bfbb36bb0c8ae45c047fc3e983 01e246ace6c3ae03

[EHEX-IMP-AK] Release vom 29.01.2026:

- Ordner “sources” unter “AK-Release 6.0.13” im Archiv:

- Name: AK-Release 6.0.13 CMS und Sourcen.zip
- SHA256: 163496d1e299e78479d08db05811f0ee4280ee5b9ffc6110beaaf043970cb48b

[ADV_IMP_eHX] Implementierungsdarstellung, Version 8.0 vom 21.08.2025, Dateiname: ADV_IMP_eHX_v8.0.xlsx

[Build_NK] SINA Buildsystem und Konnektor-Target, file name: SINA Buildsystem und Konnektor.pdf

[Build_SINA] SINA Buildenvironment: Makefiles, file name: secunet Konnektor Build-env Makefile v1.0.pdf

[NON_DEBUG] secunet Konnektor Debug vs. Non-Debug; secunet; v1.0; 26.09.2018; file name: Secunet Konnektor Debug Non-Debug v1.0.pdf

[ExtRelease] 1044_Zusatzfeatures_Extended_Release_v1.0-secunet.xlsx

[CHANGES] [CHANGES_NK]:

Modularer Konnektor 2.0.0 und 2.1.0, Risiko- und Auswirkungsanalyse (Änderungen); eHealthExperts GmbH & secunet Security Networks AG; v8.0; 27.01.2026, inklusive Patch-Dateien:

- patches-5.70.6-to-6.0.1-to-6.0.3-to-6.0.5
- patches-6.0.5-to-6.0.8-2026-01-27

[CHANGES_AK]:

- Risiko- und Auswirkungsanalyse_AK_5.70.3-5.70.5_v13.2[13]
- Risiko- und Auswirkungsanalyse_AK_5.70.5-5.70.6_v13.3[14]
- Risiko- und Auswirkungsanalyse_AK_5.70.5-6.0.5_v14.8
- Risiko- und Auswirkungsanalyse_AK_6.0.5-6.0.13_v15.3

A.3.7. **Tests (ATE)**

[ATE_FUN] Modularer Konnektor, Testkonzept; eHealthExperts GmbH & secunet Security Networks AG; v.1.2; 21.08.2018
file name: 180821_Testkonzept_v1.2.pdf

[ATE_COV] secunet(konnektor Version 2.0.0 und 2.1.0, Testabdeckung Netzkonnektor, secunet Security Networks AG, Version 1.21, 18.08.2025
file name: secunet Konnektor NK ATE_COV_v1.21.pdf

[13] Refers to a gematik minor release process performed on the base TOE

[14] Refers to a gematik minor release process performed on the base TOE

[ATE_DPT]	secunet(konnektor Version 2.0.0, 2.0.1 und 2.1.0 Testtiefe Netzkonnektor; secunet Security Networks AG; v1.14; 18.08.2025; file name: secunet Konnektor NK ATE_DPT_v1.14.pdf
[ATE_COV_AK]	secunet konnektor Version 2.0.0, 2.0.1 und 2.1.0, Testabdeckung Anwendungskonnektor, secunet Security Networks AG, Version 1.78, 06.11.2025 file name: [ATE_COV_AK] - Testabdeckung Anwendungskonnektor_V1.78.pdf
[ATE_DPT_AK]	secunet konnektor Version 2.0.0 und 2.1.0, Testtiefe Anwendungskonnektor; secunet Security Networks AG; v1.85; 25.06.2025; file name: secunet Konnektor AK ATE_DPT_v1.85_20250625.pdf
[TEST_SIG_DIR]	secunet konnektor Version 2.0.0 und 2.1.0, Testfälle Signaturdirektive, Version 1.40, 26.05.2020 filename: Testfälle _Signaturdirektive_PTV3_v140_20200526.pdf
[ATE_DokSich]	secunet konnektor Version 2.0.0 und 2.1.0, Testfälle Dokumentensicherheit, Version 1.20, 19.05.2020 filename: Testfälle_Dokumentensicherheit_PTV3_v120_20200519.pdf
[ANKE]	Beschreibung ANKE-Testumgebung Secunet Konnektor, eHealthExperts, 24.02.2022; file name: Beschreibung ANKE-Testumgebung_v3.0.pdf
[NWTU]	Netzwerktestumgebung – NWTU 1.8.0; secunet Security Networks AG; 16.11.2021; file name: Dokumentation_Netzwerktestumgebung.pdf
[VPN_TEST]	VPN –Testdurchführung in der NWTU; secunet; Version 1, 15.06.2022; filename Anleitung VPN-Tests NWTU_2022-06-15.pdf
[ANKE2]	Dokumentation Test ANKE, cons10t und ConCuTE; eHealthExperts; Version: 4.0; file name: Dokumentation Test ATE_V4.0.pdf
[ATE_Test]	secunet konnektor Version 2.0.0 und 2.1.0, Testfallspezifikationen, 01.09.2025 filename: ATE_FUN3_Testfallspezifikationen_010925_Stand_zu_6.0.5.zip
[FM-MAP]	Mapping von NFDM, AMTS Testfällen auf die Fachmodul API; eHealthExperts; v.6.0; 27.08.2025; file name: [FM_Mapping] Version 6.0.pdf
[ATE_IMP]	Test Modules Source Code; 26.06.2018; file name: SRC_cons10t.zip

[XSD] XML-Schema für die Testfallspezifikation; v1.0;
file name: s10.xsd

[ATE_REPORT] Testberichte:
- HTML-Report_6.0.5_mit_Logs_01.zip (25.08.2025)
- HTML-Report_6.0.8_mit_Logs_01.zip (05.02.2026)

[ATE_IAR_6.0.8] Ergänzende Tests zur Auswirkungsanalyse des NK in Version 6.0.8, TestartefakteZumIarNK6.0.8.tar.gz, 03.02.2026

[ATE_IAR_6.0.13] Ergänzende Dokumentation der Risiko- und Auswirkungsanalyse (Änderungen) AK bzgl. Testung der Anpassungen Test_Änderungen_AK_6.0.5-6.0.13.pdf, Version 1.0, 04.02.2026

A.3.8. **Life Cycle (ALC)**

A.3.8.1. **ALC – secunet**

[ALC_CMC] secunet Konnektor (PTV3) Version 2.0.0 und 2.1.0, Konfigurationsmanagement (ALC_CMC.4), Version 1.0, 12.11.2024

[ALC_CMS] see [ALC_CMS_NK] and [ALC_CMS_AK] and bibliography document: 1209-V3_1044-V9_References_secunet_konnektor v1.28.pdf

[ALC_CMS_NK] From [SECU-IMP-NK] archive:

- files: connector-all-components.csv and konnektor-alc_cms.csv

[ALC_DEL] secunet(konnektor Version 2.0.0 und 2.1.0, Auslieferung (ALC_DEL.1), Version 1.0, 05.03.2025

[ALC_DEL2] secunet(konnektor Version 2.0.0, 2.0.1 und 2.1.0, Hinweise zur sicheren Lagerung und Lieferkette, Version 2.1, 11.05.2023

[ALC_DVS] secunet(konnektor Version 2.0.0 und 2.1.0, Sicherheit bei der Entwicklung (ALC_DVS.1), Version 1.24, 28.07.2025

[ALC_FLR] secunet(konnektor Version 2.0.0 und 2.1.0, Fehlerbehebung (ALC_FLR.2), Version 1.0, 05.03.2025

[ALC_LCD] secunet(konnektor Version 2.0.0 und 2.1.0, Lebenszyklus-Beschreibung (ALC_LCD.1), Version 1.0, 06.03.2025

[ALC_TAT] secunet Konnektor Version 2.0.0 und 2.1.0, Werkzeuge und Techniken (ALC_TAT.1), Version 2.1, 06.08.2025

[CodeImport] Modularer Konnektor, Code-Überführung, Version 1.0 vom 28.10.2019 und [CodeImport_eHx]

[JIRA-CERT-Admin] secunet Konnektor Version 2.0.0 und 2.1.0, Jira CERT Administrator-Handbuch, Version 1.4, 12.07.2022

[JIRA-CERT-Product] secunet Konnektor Version 2.0.0 und 2.1.0, Jira CERT Produktmanager, Produktentwickler, JIRA Cert Bewerter, Version 1.3, 12.07.2022

[JIRA-CERT-Incident] secunet Konnektor Version 2.0.0 und 2.1.0, Jira CERT Incident Manager, Version 1.2, 12.07.2022

[JIRA-Kollab] secunet(konnektor, JIRA-Kollab, Version 1.1, 11.06.2025

[DPFlow1] Daten und Prozess Fluss secunet(konnektor Anhang A zu ALC_DEL, ALC_LCD, Version 0.93, 03.05.2018, filename: 20180503_Daten_und_Prozess_Fluss_secunetkonnektor_Anhang_A_ALC_DEL_LCD_v0.93.pdf

[DPFlow2] secunet(konnektor Datenfluss ALC_CMC, Version 0.93, 27.08.2019, filename: 20190827_Datenfluss_0.93_ALC_CMC.pdf

[DPFlow3] PCBA Vorbereitung zur optischen Inspektion ALC_DVS, Version 0.91, 02.11.2017,
file name: 20171102_Optische_Inspektion_0.91_ALC_DVS.pdf

[DPFlow4] secunet(konnektor Prozessdiagramm finale Montage, Version 0.92, 06.03.2018,
file name: 20180306_Prozessflow_TOE_Produktion_0.92_ALC_LCD.pdf

[ALC_Sites] Anlage Standorte zum Antrag auf eine Produktzertifizierung für den secunet eHealth konnektor 2.0.0, 2.0.1 und 2.1.0, 07.03.2024

[SLA_Log] Anlage 5 – Service Level Anforderungen (SLA) und Logistik, Version: 1, 07.02.2018

[KeyList] secunet konnektor Version 2.0.0, Key Liste, Version 0.91, 23.02.2018

[KeyMgmt] secunet(konnektor Version 2.0.0, Schlüsselmanagementkonzept Boot Guard, BIOS und Secure Boot, Version 1.0, 22.10.18

[KeyKnzpt] secunet(konnektor, Modularer Konnektor Version 2.0, Schlüssel-konzept, Version 1.1, 14.08.2025

[KeyProt] Schlüsselmanagementkonzept Boot Guard und BIOS, Anhang A, Ablaufprotokoll vom 13.02.2018

[RL_ZUT] secunet, ISMS – Richtlinie, Zutrittsrichtlinie, Version 2.1, 01.07.2025

[RL_MOB] [ALC_MOR]: Mobile Office Richtlinie mit Anlagen zum Shared Desk Konzept und Working, Remote Konzepts des secunet Konzerns, Version 3.0, 19.02.2025

[DevGuide] Entwicklerhandbuch Modularer Konnektor, secunet AK-Anteil, Version 1.0, 05.03.2025

A.3.8.2. **ALC - eHealth Experts**

[ALC_CMC_eHX] eHealthExperts EHX Group, ALC_CMC.4, Konfiguartionsmanagement, Version 2.3, 16.03.2021

[ALC_CMS_AK] From [EHEX-IMP-AK]

- file: ALC_CMS_eHX_v<xyz>.xlsx

[ALC_DEL_eHX] eHealthExperts EHX Group, ALC_DEL.1, Anwendungskonnektor, Version 1.0, 21.06.2018

[ALC_DVS_eHX] eHealthExperts EHX Group, Sicherheitskonzept (ALC_DVS.1), Anwendungskonnektor, Version 3.4, 23.07.2025

[ALC_FLR_eHX] eHealthExperts EHX Group, Fehlerbehebung (ALC_FLR.2), Anwendungskonnektor, Version 3.0, 04.08.2022

[ALC_LCD_eHX] eHealthExperts EHX Group, Lebenszyklus-Beschreibung (ALC_LCD.1), Anwendungskonnektor, Version 3.0, 04.08.2022

[ALC_TAT_eHX] eHealthExperts, EHX Group, ALC_TAT.1, Anwendungskonnektor, Version 2.6, 26.11.2024

[CodeImport_eHx] Anleitung Code-Überführung, Version 1.3, 11.03.2021

A.3.8.3. **ALC – S.I.E**

[ALC_CMC_SIE] Konfigurationssmanagementsystem (ALC_CMC), Regulatory Affairs Document, S.I.E., 5.0.0, 07.03.2023

[ALC_CMS_SIE] Konfigurationsliste (ALC_CMS), Regulatory Affairs Document, S.I.E, Rev# 6.0.0, 27.02.2025

[ALC_DVS_SIE] Sicherheitsmaßnahmen der TOE-Produktion (ALC_DVS), Regulatory Affairs Document, S.I.E, Rev# 4.0.0, 24.03.2023

[ALC_LCD_SIE] Life-cycle des TOE (ALC_LCD), Regulatory Affairs Document, S.I.E, Rev# 6.00, 24.03.2023

[ALC_TAT_SIE] Tools and techniques (ALC_TAT), Regulatory Affairs Document, S.I.E., Rev# 2.0.0, 07.03.2023

A.3.8.4. **ALC – Audit Evidences**

A.3.8.4.1. **([Evidence-E]) Audit evidence secunet (Essen)**

[Audit-E_01] CVE Analyse nur in Räumlichkeiten der Konnektor-Entwicklung.msg
Richtlinie für die Softwareentwicklung im Rahmen des Konnektorprojektes-v10-Export_2025_08_04.pdf

[Audit-E_02] RL-Alarmprozesse_Merkblatt_Alarmkontakt.pdf
RL-Alarmprozesse_Merkblatt_Meldestelle.pdf
RL-Alarmprozesse_Merkblatt_Wachdienst.pdf

[Audit-E_03] proj-konnektor.secunet.de_ Backup-v7-20250725_221111-1.pdf
Rackchecker Essen-v10-20250725_221723.pdf

[Audit-E_04] Rackchecker_Netzplan_v1.1.pdf

A.3.8.4.2. **([Evidence-DD]) Audit evidence secunet (Dresden)**

[Audit-DD_01] Power_Alarmueberwachungsvertrag.pdf
Änderung im Alarmüberwachungsvertrag.pdf

A.3.8.4.3. **([Evidence-B1]) Audit evidence eHealth Experts Berlin**

[Audit-B1_01] A.1_Umgang-mit-CVEs.pdf

[Audit-B1_02] APD-100 Datenblatt.pdf
APD-100.jpg

A.3.8.4.4. **([Evidence-B2]) Audit evidence secunet Berlin**

[Audit-B2_01] Same as [Audit-E_01]

[Audit-B2_02] Netzplan Berlin.pdf

A.3.8.4.5. **([Evidence-L]) Audit evidence S.I.E Lustenau (Austria)**

[Audit-L_01] Auszug aus „Zutrittsrichtlinie“, A.1.png

[Audit-L_02] Auszug aus „S.I.E Offboarding IT„, A.3.png

[Audit-L_03] 2025-05-21_Instandhaltungsprotokoll_Alarm_61335818.pdf
2025-05-21_Instandhaltungsprotokoll_Video_61336770.pdf

[Audit-L_04] Auszug aus „Zutrittsrichtlinie“, C.2.png

[Audit-L_05] Auszug aus „Recruiting“, C.3.png

A.4. Single Evaluation Reports

A.4.1. **ASE**

[SER_ASE] Single Evaluation Report CC Aspect ASE, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1209-V3, Version 3.3, 08.09.2025, SRC Security Research & Consulting GmbH,
file name: 1209-V3_ASE_250908_v33.pdf

Single Evaluation Report CC Aspect ASE, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.1, 08.09.2025, SRC Security Research & Consulting GmbH,
file name: 1044-V9_ASE_250908_v21.pdf

A.4.2. **AGD and ADV**

[SER_AGD-ADV] Single Evaluation Report CC Aspect AGD-ADV, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 3.0, 08.09.2025, SRC Security Research & Consulting GmbH,
file name: 1209-V3_AGD-ADV_250908_v30.pdf

[SER_ADV] Single Evaluation Report CC Aspect ADV, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.7, 08.09.2025, SRC Security Research & Consulting GmbH,
file name: 1209-V3_ADV_250908_v27.pdf

[SER_ADV_RNG] Evaluation Report as part of the Evaluation Technical Report, Part B, ETR-Part Deterministic Random Number Generator, BSI-DSZ-CC-1044-V8, BSI-DSZ-CC-1209-V2,
file name: 1209-V2_ADV_RNG_250404_v04

[KERNEL_REVIEW] Bewertung der Konnektor Kernelkonfiguration; SRC; v3.3; 14.01.2021
file name: PTV4_ARC_KernelKonfig_210114_v33.xlsx

A.4.3. **ALC**

[SER_ALC] Single Evaluation Report CC Aspect ALC, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 2.1, 19.09.2025, SRC Security Research & Consulting GmbH,
file name: 1209-V3_ALC_250919_v21.pdf

[ChkL_Sec-Dresden] Checklist of the Audit at secunet Security Networks AG in Dresden, Germany, on 26.06.2025, in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.0, 25.05.2025, file name: 1209-V3_ALC_AuditChklist_SecunetDresden_20250525_v10

[ChkL_Sec-Essen] Checklist of the Audit at secunet Security Networks AG in Essen, Germany, on 17.06.2025, in the context of the evaluation of the secunet

konnektor 2.0.0 and 2.1.0, Version 1.1, 11.0.6.2025, file name: 1209-V3_ALC_AuditChklist_SecunetEssen_250611_v11

[ChkL_eHX-Berlin] Checklist of the Audit at eHealth Experts in Berlin, Germany, on 24.06.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.0, 25.05.2025, file name: 1209-V3_ALC_AuditChklist_eHXBerlin_20250525_v10

[ChkL_Sec-Berlin] Checklist of the Audit at secunet Security Networks AG in Berlin, Germany, on 25.06.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.0, 25.05.2025, file name: 1209-V3_ALC_AuditChklist_SecunetBerlin_20250525_v10

[ChkL_SIE-Lustenau] Checklist of the Audit at S.I.E Solutions in Lustenau, Austria, on 24.07.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.0, 23.05.2025, file name: 1209-V3_ALC_AuditChklist_SIE_Lustenau_20250523_v10

[Protocol_D] Protocol of the Audit at secunet Security Networks AG in Dresden, Germany, on 26.06.2025, in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.2, 10.07.2025

[Protocol_E] Protocol of the Audit at secunet Security Networks AG in Essen, Germany, on 17.06.2025, in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.3, 08.07.2025

[Protocol_B1] Protocol of the Audit at eHealth Experts in Berlin, Germany, on 24.06.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.2, 10.07.2025

[Protocol_B2] Protocol of the Audit at secunet Security Networks AG in Berlin, Germany, on 25.06.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.2, 10.07.2025

[Protocol_L] Protocol of the Audit at S.I.E Solutions in Lustenau, Austria, on 24.07.2025 in the context of the evaluation of the secunet konnektor 2.0.0 and 2.1.0, Version 1.2, 05.08.2025

[Findings_DD] List of findings during the audit on 2025-06-26 at secunet AG (secunet), Dresden, version 1.3, 06.08.2025

[Findings_E] List of findings during the audit from 2025-06-17 at secunet (secunet), Essen, Version 1.3, 06.08.2025

[Findings_B1] List of findings during the audit on 2025-06-24 at eHealth Experts (eHX), Berlin, Version 1.3, 06.08.2025

[Findings_B2] List of findings during the audit on 2025-06-2025 at secunet (secunet), Berlin, Version 1.3, 06.08.2025

[Findings_L] List of findings during the audit on 2025-07-24 at System Industrie Electronic GmbH (SIE), A-Lustenau, Version 1.3, 17.09.2025

A.4.4. **ATE**

[SER_ATE] Single Evaluation Report CC Assurance Class ATE, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9, Version 3.4, 10.02.2026, SRC Security Research & Consulting GmbH,
file name: 1209-V3_ATE_260210_v34.pdf

[ATE_IND] Combined reference for [ATE_IND_NK] and [ATE_IND_AK]

[ATE_IND_AK] ATE Independent Testing AK, secunet konnektor 2.0.0 and 2.1.0; SRC; Version 0.8; 11.02.2022, SRC Security Research & Consulting GmbH;
file name: 1184_ATE_IND_AK_220211_v08.pdf

[ATE_IND_NK] ATE Independent Testing NK, secunet konnektor 2.0.0 and 2.1.0; SRC; Version 1.2; 11.02.2022, SRC Security Research & Consulting GmbH;
file name: 1184_ATE_IND_NK_220211_v12.pdf

[TLS_Tests] Evaluator-Tests regarding TLS Testing, Version 1.5, 26.08.2025, SRC Security Research & Consulting GmbH
file name: 1209-V3_AVA_TLS_Testing_250826_v15.pdf

[VPN_Tests] Evaluator-Tests regarding IPsec Testing, Version 0.9, 08.08.2022, SRC Security Research & Consulting GmbH
file name: 1201_IPsec_Testing_2200808_v09.pdf

[ATE_Infomodel] Info Model in the ANKE Test Environment, Evaluation of CC Assurance Class ATE (Info Model), Version 1.1, 19.05.2020
file name: 1135_ATE_Default_Infomodel_200519_v11.pdf

[Tests_FDP_ACF] Testabdeckung FDP_ACF; SRC; Version 1.7, 11.02.2022;
file name: 1184_ATE_Testabdeckung FDP_ACF_220211_v17

[ATE_IND_DEV] Testlogs of ATE_IND evaluator sample from developer tests, file name: NWTU_test_20250905.zip

[TLS_ConfChk] Evidenzen gesammelt im Rahmen der Konfigurationschecks zu TLS:

- PTV5 WR3 (BSI-DSZ-CC-1209-2023): TLS_ConfChk_20230713.zip
- PTV5 WR4 (BSI-DSZ-CC-1209-V2): TLS_Conf-Chk_20250117.zip

[VPN_ConfChk] Evidenzen gesammelt im Rahmen der Konfigurationschecks zu IKE/IP-Sec:

- PTV5 WR3 (BSI-DSZ-CC-1209-2023):
  VPN_ConfChk_20230627.zip

[FW_ConfChk] Evidenzen gesammelt im Rahmen der Konfigurationschecks zur Firewall:

- PTV5 WR3 (BSI-DSZ-CC-1209-2023):
  FW_ConfChk_20230615.zip
- PTV6 (BSI-DSZ-CC-1209-V3)
  FW_ConfChk_20260202.zip

A.4.5. **AVA**

[AVA_Testplan] Test plan for secunet konnektor 2.0.0 2.1.0, BSI-DSZ-CC-1209-V3 et al., version 0.1, 07.07.2025, file name: 1209-V3_Testplan_250707_v01

[SER_AVA] Single Evaluation Report CC Assurance Class AVA, secunet konnektor 2.0.0 und 2.1.0, Certification ID BSI-DSZ-CC-1044-V9 et al., Version 3.5, 19.11.2025, SRC Security Research & Consulting GmbH, file name: 1209-V3_AVA_251119_v35.pdf

[AVA_OS] AVA Operating System secunet konnektor v2.0.0 and v2.1.0, Version 1.5, 23.12.2021, SRC Security Research & Consulting GmbH
file name: 1184_AVA_OS_211223_v15.pdf
including Logs: FW5.0.4_AVA_OS_Logs_20211223.zip

[AVA_CCA] Cryptographic conformity assessment - Kryptographische Mechanismen des secunet eHealth konnektor 2.0.0 und 2.1.0 (PTV6), Version 1.1, 18.09.2025, file name: 1209-V3_AVA_CCA_250918_v11

[ARC_BIOS] Checkliste zur Prüfung der Implementierung von secunet Konnektor (CSAS Mainboard): Härtungsmaßnahmen und sicherer Start-up der Firmware“, Version 0.4, 23.03.2018.

[TLS_Analysis] TLS Analyse secunet konnektor, Version 2.0.0, Anforderungen an TLS im deutschen CC-Zertifizierungsschema, SRC Security Research & Consulting GmbH Version 2.0; 31.07.2025;
file name: 1209-V3_AVA_TLS_Analysis_20250731_v20.pdf

[VPN_Analysis] [VPN_Analysis1]:
VPN Analyse, Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, SRC Security Research & Consulting GmbH, Version 1.5, 10.07.2025
file name: 1209-V3_AVA_VPN_Analysis_250710_v15.pdf

[VPN_Analysis2]:
IPsec-RFCs - MAY_SHOULD Anforderungen; SRC Security Research & Consulting GmbH; Version 0.6; 10.07.2025;
file name: 1209-V3_AVA_VPN_Analysis_RFCMS_250710_v06

[CVE_analysis_evaluator]	AVA CVE Analysis Evaluator secunet konnektor 2.0.0 und 2.1.0, Version 28.01.2026, SRC Security Research & Consulting GmbH file name: 1209-V3_AVA_CVE_Analysis_260128_v19.pdf Including sub-files: [CVE_Result_NK] - 20251115_cves_details_20251111_toollist_NK_20250919_full.xlsx - 20260127_cves_details_20260127_toollist_NK_20250919_a20251111_full.xlsx - 20260130_cves_details_20260127_toollist_NK_20250919_BSI_OpenSSL_CVEs_full.xlsx [CVE_Result_AK] - 20251115_cves_details_20251111_toollist_AK_20250919_full.xlsx.xlsx - 20260127_cves_details_20260127_toollist_AK_20250919_a20251111_full.xlsx
[Zert_Analysis]	Analyse zum Zertifikatsdienst des Konnektors, SRC Security Research & Consulting GmbH, Version 1.6, 11.07.2025 file name: 1209-V3_AVA_Zert_Analysis_250711_v16.pdf
[Network_PEN_Testing]	Bericht über das Netzwerkpentesting am Secunet Konnektor, Zertifizierungs-ID: BSI-DSZ-CC-1209-V3 et al., SRC Security Research & Consulting GmbH, Version 1.7, 17.10.2025, file name: 1209-V3_Pentestbericht_Secunet_251017_v17
[analysis_firewall_rules]	Prüfung der Paketfilterregeln secunet konnektor 2.0.0, Version 1.6, 19.11.2021, file name: 1184_FWReview_211119_v16.pdf Inkludiert [FWReview-Table] mit Details, Version 1.6, 19.11.2021, file name: 1184_FWReviewTable_20211119_v16 und FW5.0.3_config_2021-11-19_111404
[firewall_tests]	Evaluator-Tests der Firewall, Version 0.6, 19.11.2021, file name: 1184_FW_Tests_211119_v06.pdf Inkludiert [fw_tests_logs] Logs der Firewall-Tests in [firewall_tests] file name: FW5.0.3_FW_tests_logs_20211119.zip

[static_code_analysis]	Static Source Code Analysis secunet konnektor v2.0.0, SRC Security Research & Consulting GmbH, Version 1.4, 10.02.2022, file name: 1184_SSCA_220210_v14
[vpn_load_test]	Lasttests secunet konnektor 2.0.0, SRC Security Research & Consulting GmbH, Version 1.1, 23.11.2021 file name: 1184_VPN_Lasttests_211123_v11.pdf
[BSI_Liste_analysis]	Dieses Dokument ist ein in Excel konvertiertes Dokument [BSI_Liste], welches die Analyseergebnisse der Prüfstelle dokumententiert, file name: 1209-V3_Evaluierungshinweise_2021-11-19_250708_v01
[PDF_Attacks]	Webseite: https://www.pdf-insecurity.org/pdf-dangerous-paths/attacks.html, Stand 06.05.2021, file name: PDF Insecurity Website_20210506.zip

A.5. Weitere Dokumente

[VPN-Szenarien]	Sieben Szenarien zur Berücksichtigung bei den Penetrationstests der VPN-Kanäle des Netzkonnektors in der Fassung vom 24.08.2018, übermittelt durch die Zertifzierungsstelle file name: Angriffsszenarien.2018-08-24.odt
[BSI-OpenSSL-1]	Quellcode-basierte Untersuchung von kryptographisch relevanten Aspekten der OpenSSL-Bibliothek, eine Studie im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik, Version 1.0.1, 03.11.2015
[TLS_Anf]	Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-Zertifizierungsschema, Version 0.02, 18.01.2016, BSI
[VPN_Anf]	Anforderungen an kryptographisch gesicherte VPN-Kanäle / Trusted Channels im deutschen CC-ZertifizierungsschemaIKE/ IPsec, Version 0.01, 16.02.2015, BSI
[N4200]	Intel® Pentium® Prozessor N4200; Intel Corporation; file name: https://ark.intel.com/de/products/95592/Intel-Pentium-Processor-N4200-2M-Cache-up-to-2_5-GHz
[INTEL64]	Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2B: Instruction Set Reference, M-U; Order Number: 253667-060US; September 2016 file name: https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-vol-2b-manual.pdf

[JAVA_SEC_CODE] file name: https://www.oracle.com/technetwork/java/seccode-guide-139067.html

[JIL AttMeth] Attack Methods for POIs, Version 1.95, February 2015, Joint Interpretation Library (JIL) / JIWG

[BSI_Liste] Konnektor-Evaluierung, Dokument: Konnektor_Evaluierungshinweise_mAe__Nov_2021.odt

[ETR_RZK_1128] Evaluation Report, Evaluation Technical Report (ETR), Version: Version 1.3, Date: 19.11.2019, BSI-DSZ-CC-1128, SRC Security Research & Consulting GmbH

[BSI_Liste_LZV] Laufzeitverlängerung (LZV): Zu berücksichtigende Aspekte (Version 1.1 vom 02.08.2023 aus Mial vom 03.08.2023), file name: CheckListe_LZV.docx

[BSI_Liste_LZV_Analyse] Ergebnisse zur Prüfung der speziellen Aspekte der Laufzeitverlängerung im Verfahren BSI-DSZ-CC-1209 et al. (Version 1 vom 18.08.2023), file name: CheckListe_LZV-summary_20230818_v1.pdf

[BSI_RNG] Evaluierung von NIST SP 800-90A DRBGs, Referat S 24.

[JIL_CrisisPol] JIL Crisis Policy, Dated: October 2023, Approved: November 2023, Version: 1.0

[KickOff_1209-V2] SRC protocol: KickOff am 24.03.2025; 10:15 – 12:00, Re-Zertifizierung zum Verfahren BSI-DSZ-CC-1209-V2-2025 (noch in Zertifizierung inkl. des NK Parallelverfahren BSI-DSZ-CC-1044-V8-2025) zu secunet konnektor 2.0.0 und secunet konnektor 2.1.0 von secunet Security Networks, file name: secunet-2410_PTV6_KickOff_20250324_v1

BSI protocol: Protokoll zum Kick-Off-Meeting, Version: [V3], Erstellungsdatum: 24.03.2025, Dateiname: 20250324_Protokoll_Kickoff_Secunet.docx, Betreff: Kick-Off-Telefonkonferenz am 09.09.2024, Beantragtes Verfahren: Re-Zertifizierung, Produkt: secunet konnektor 2.0.0, Version 6.0.0:2.0.0, secunet konnektor 2.1.0, Version 6.0.0:2.1.0, Antragsteller: secunet Security Networks AG, Prüfstelle: SRC Security Research & Consulting GmbH