Security Target für RISE-Konnektor V6.0

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F
2320 Schwechat
Austria (Europe)
Tel: +43 1 9049007-0
E-Mail: welcome@rise-world.com
Internet: https://www.rise-world.com

Änderungsverlauf

Version	Datum	Änderungen	Anmerkungen
1.9	31.10.2018	Finalisierung	ST zur Veröffentlichung bestimmt
2.0	29.05.2019	Aufbereitung für Re-Zertifizierung	Vorversion 1.9 dieses Dokuments entspricht der veröffentlichen Version zum Zertifikat BSI-DSZ-CC-1052
2.1	03.06.2019	Anpassung wg. AutoUpdate	
2.11	30.10.2019	editorielle Anpassungen	
2.12	22.11.2019	Anpassungen nach ASE-Evaluierung	
3.0	29.10.2020	Aktualisierung des PP-0097 eingepflegt Anpassung an neue FW-Version	
3.1	24.11.2020	TLS-Authentisierungsalgorithmen ergänzt	ST zur Veröffentlichung bestimmt
3.11	12.01.2021	Firmwareversion inkrementiert	ST zur Veröffentlichung bestimmt
4.0	18.05.2021	Update für PTV4	ST zur Veröffentlichung bestimmt
4.1	31.10.2021	Update für PTV5	ST zur Vorlage beim BSI
4.2	12.01.2022	Anpassung Tabelle 1	
5.0	22.09.2023	Update für PTV5M	ST zur Vorlage beim BSI
5.1	12.01.2024	Versionsupdate für RISE-Konnektor V5.2	
6.0.0	15.01.2025	Versionsupdate für RISE Konnektor V6.0	
6.0.1	21.03.2025	Update Firmware-Version	
6.0.2	27.03.2025	Entfernen FM ePA in Darstellungen, Anpassung [16]	
6.0.3	22.04.2025	Anpassung FW- und Fachmodul-Versionen	
6.0.4	12.05.2025	Entfernen PRF_HMAC_SHA1, TLS_ECDHE_RSA_WITH_A	

Version	Datum	Änderungen	Anmerkungen
		ES_256_CBC_SHA und TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	
6.0.5	17.06.2025	Redaktionelle Korrekturen	
6.0.6	05.08.2025	Redaktionelle Korrekturen	
6.0.7	06.08.2025	Redaktionelle Korrekturen	
6.0.8	07.08.2025	Redaktionelle Korrekturen	
6.0.9	29.10.2025	Anpassungen nach Rückmeldung BSI	

Inhaltsverzeichnis

1. ST-Einführung

1.1. ST und EVG Referenz

Titel:	Security Target für RISE-Konnektor V6.0
Version:	6.0.9
Datum:	29.10.2025
Allgemeiner Status:	abgeschlossen
Zertifizierungs ID:	BSI-DSZ-CC-1052-V6
PP Registrierung:	BSI-CC-PP-0097-V2-2020-MA-02
PP Registrierung bei:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC-Version	3.1 (Revision 5)
Vertrauenswürdigkeitsstufe:	EAL3 erweitert um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5 und ALC_FLR.2
Verfasser:	SRC GmbH / Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
EVG Name.	RISE-Konnektor V6.0
EVG Version	V6.0
Stichwörter:	Konnektor, Netzkonnektor, eHealth, elektronisches Gesundheitswesen, Telematikinfrastruktur, dezentrale Komponente

Dieses Dokument orientiert sich in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang in Abschnitt 8 (insbesondere Abschnitt 8.6.4) aufgeführt sind; allen voran die Konnektorspezifikation:

[16] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon],

1.2. EVG-Übersicht

Dieses Security Target beschreibt den Schutzbedarf für einen Netzkonnektor als Bestandteil des Konnektors im Gesundheitswesen gemäß Spezifikation [16].

Der Konnektor besteht aus dem Netzkonnektor (NK), dem Anwendungskonnektor (AK) und der Security Module Card Konnektor (gSMC-K). Er stellt die Plattform für die Ausführung von Fachmodulen bereit. Der Netzkonnektor stellt Paketfilter- und VPN-Funktionalität für die Kommunikation mit der zentralen Telematikinfrastruktur-Plattform und einem Sicheren Internet Service (SIS) bereit, ebenso die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und fachanwendungsspezifischen Diensten (Fachdiensten bzw. Intermediären). Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssytem und dem Objektsystem für gSMC-K. Sie speichert Schlüsselmaterial für den Netzkonnektor und den Anwendungskonnektor und stellt kryptographische Sicherheitsfunktionen bereit. Die Sicherheitsfunktionalität des Anwendungskonnektors umfasst die Signaturanwendung, die Verschlüsselung und Entschlüsselung von Dokumenten, den Kartenterminaldienst und den Chipkartendienst.

1.2.1. Abgrenzung

Das Schutzprofil BSI-CC-PP-0098-V3-2021-MA-03 [12] definiert die Sicherheitsanforderungen an den Konnektor, wobei die gSMC-K separat betrachtet wird: Das Chipkartenbetriebssytem der gSMC-K und das Objektsystem der gSMC-K sind durch die gematik zugelassen.

Der EVG des vorliegenden ST basiert auf dem Schutzprofil BSI-CC-PP-0097-V2-2020-MA-02 und schließt die gSMC-K als Teil der IT-Umgebung ein. Die relevanten Sicherheitsziele der Einsatzumgebung, wie OE.NK.gSMC-K, OE.NK.KeyStorage und ggf. OE.NK.RNG beziehen sich auf die Funktionalität der gSMC-K.

Die Konnektorspezifikation [16] definiert ein Konnektormanagement, das Sicherheitsfunktionalität umfasst, die keiner speziellen Komponente des Konnektors zugeordnet wird und folglich auch für die den Netzkonnektor betreffenden Aspekte durch den Netzkonnektor selbst erbracht werden kann. Das betrifft das Konnektormanagement mit

- der Managementschnittstelle,
- der Benutzerverwaltung,
- dem Management der Konfigurationsdaten,
- der Administration der Fachmodule,
- der Software-Aktualisierung (KSR-Client),
- dem Werksreset, und
- der In- und Außerbetriebnahme des Konnektors.

Für diese Funktionalität wird auf das Schutzprofil BSI-CC-PP-0098-V3-2021-MA-03 [12] mit den Sicherheitsanforderungen an den Konnektor (ohne gSMC-K) verwiesen.

1.2.2. Terminologie

Zum zugrunde liegendenen Schutzprofil konforme Produkte werden als Netzkonnektor bezeichnet und im Folgenden „Evaluierungsgegenstand“ (EVG, englisch „Target of Evaluation“, TOE) genannt.

Der Konnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens[1] und den Clientsystemen der Leistungserbringer. Die Chipkarten elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA), die Institutionskarte SM-B[2] (SMC-B oder HSM-B), die Kartenterminals und die Konnektoren bilden die dezentralen Komponenten der Telematikinfrastruktur. Zu den Clientsystemen gehören die Praxisverwaltungssysteme der Ärzte (PVS), die Krankenhausinformationssysteme (KIS) und die Apothekenverwaltungssysteme (AVS). Der Konnektor stellt auch eine gesicherte Verbindung zu einem Sicheren Internet Server (SIS) bereit.

1.3. EVG-Beschreibung

Der Evaluierungsgegenstand (EVG) ist der Netzkonnektor gemäß der Abgrenzung in BSI-CC-PP-0097-V2-2020-MA-02 und umfasst folgende Anteile:

- Software des Netzkonnektors;

Die folgenden Konnektoranteile sind nicht Bestandteil des EVG:

- Software des Anwendungskonnektors;
- Software des Fachmoduls VSDM;
- Hardware inkl. BIOS;
- Software des Fachmoduls AMTS;
- Software des Fachmoduls NFDM;

Der Konnektor wird als eine Einbox-Lösung implementiert. Das Gerät, das den EVG beinhaltet, ist in einem quaderförmigen Gehäuse untergebracht, und verfügt über die Hardwareanschlüsse, die für den Betrieb des Konnektors nötig sind. Die gSMC-Ks (vgl. Abschnitt 1.3.6) befinden sich ebenfalls in diesem Gehäuse.

---

[1] Ein Glossar der wichtigsten Begriffe befindet sich im Anhang in Abschnitt 8.3. Für Fachtermini der elektronischen Gesundheitskarte und der Telematikinfrastruktur des Gesundheitswesens wird darüber hinaus auf die Seiten des Bundesministeriums für Gesundheit (BMG, https://www.bmg.bund.de), der GmbH (gematik, https://www.gematik.de) und des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI, https://www.dimdi.de) verwiesen. Das Projekt-Glossar der gematik wird unter gemSpec_Kon [16] referenziert.

[2] Die Institutionskarte SM-B ist ein zusammenfassender Begriff für eine SMC-B (Security Module Card Typ B), als auch eine in einem HSM-B (HSM-Variante einer Institutionskarte Typ B) enthaltene virtuelle SMC-B

Der EVG RISE-Konnektor V6.0 besteht aus folgenden Teilkomponenten und wird ausschließlich mit der genannten Hardwareversion ausgeliefert:

Komponenten	**Version**
Software des Konnektors (Netzkonnektor, Anwendungskonnektor sowie Fachmodul VSDM)	5.6.2
Fachmodul AMTS *(nicht Teil des EVG)*	1.2.1
Fachmodul NFDM *(nicht Teil des EVG)*	1.2.1
Hardware inkl. BIOS (nicht Teil des EVG)	*1.0.0*

Tabelle 2: Komponenten der Einbox-Lösung

Das Gerät wird über eine Lieferkette dem Endkunden (Leistungserbringer) zugestellt. Die Sicherheit der Lieferkette wird durch die Vertrauenswürdigkeitskomponente ALC_DEL.1 gewährleistet, vgl. auch Abschnitt 6.3.1. Die Anweisungen an den Nutzer, wie die Einhaltung der sicheren Lieferkette überprüft werden kann, sind auch im Benutzerhandbuch enthalten.

Der Lieferumfang des EVG umfasst ebenfalls die Betriebsdokumentation für den Konnektor, die in elektronischer Form dem Endkunden bereitgestellt wird:

- RISE Konnektor Bedienungsanleitung, [RISE-KON-AGD_OPE];

Im Zertifizierungsreport, der nach Abschluss der Evaluierung ebenso wie diese Sicherheitsvorgaben auf der Internetpräsenz[3] des Bundesamts für Sicherheit in der Informationstechnik (BSI) veröffentlicht wird, ist der Hashwert des Handbuchs genannt. Dieser Hashwert gibt dem Endkunden die Möglichkeit, die Integrität und Authentizität des Handbuchs zu verifizieren.

1.3.1. EVG-Typ

Der EVG ist ein Produkt. Er umfasst die Sicherheitsfunktionalität einer Firewall, eines VPN-Clients sowie von Servern für einen Zeitdienst, einen Namensdienst (DNS) und einen DHCP-Dienst. Zudem beinhaltet es die Basisfunktionen zum Aufbau von TLS-Kanälen zu anderen IT-Produkten.

Der Konnektor stellt einen neuen Produkttyp dar, so dass außer dem Gattungsbegriff „Konnektor“ kein weiterer EVG-Typ benannt werden kann.

Die Verantwortung für den Betrieb des Netzkonnektors liegt beim Konnektor-Betreiber (bzw. Leistungserbringer); der Netzkonnektor stellt jedoch ein Zugangserfordernis zur Telematikinfrastruktur dar und es dürfen nur von der gematik zugelassene und geprüfte Konnektoren eingesetzt werden.

[3] https://www.bsi.bund.de/

Der Konnektor erbringt Sicherheitsleistungen in drei wesentlichen Funktionsblöcken: Netzkonnektor, Anwendungskonnektor und Sicherheitsmodul.

- Die Sicherheitsfunktionalität einer Firewall, eines VPN-Clients, und von Servern für Zeitdienst, Namensdienst und DHCP-Dienst werden durch den Bestandteil Netzkonnektor (EVG) erbracht, ebenso die Basisdienste zum Aufbau von TLS-Kanälen.

- Die Sicherheitsfunktionalität einer Signaturanwendung, eines Kryptomoduls für die Verschlüsselung und für die Initiierung der gesicherten Kommunikation zwischen dem Konnektor und dem Clientsystem, zwischen Fachmodulen und Fachdiensten sowie zwischen Servern und dem Kartenterminaldienst, dem Chipkartendienst, werden durch den Anwendungskonnektors erbracht.

- Das Sicherheitsmodul gSMC-K stellt interne Sicherheitsfunktionalität zur Speicherung von Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit.

In diesem ST werden nur die vom Netzkonnektor erbrachten Sicherheitsleistungen betrachtet. Der Anwendungskonnektor und das Sicherheitsmodul werden als Teil der Einsatzumgebung betrachtet.

Die wesentlichen Funktionsblöcke des Konnektors sind in der folgenden Abbildung 1 dargestellt.

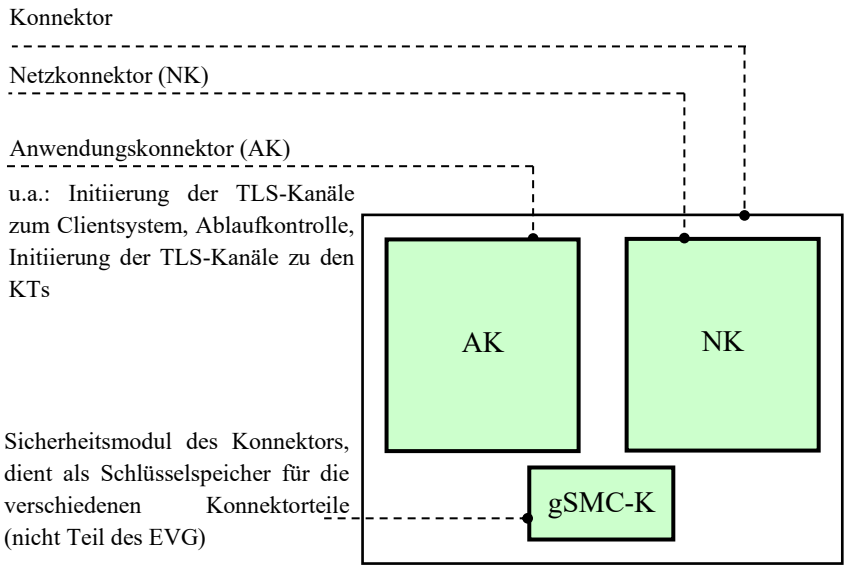

Abbildung 1: Funktionsblöcke des Konnektors

Firewall

Der Netzkonnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens (außerhalb der Verantwortlichkeit der Leistungserbringer) und den dezentralen Systemen. Er stellt den netzseitigen Abschluss der zentralen Telematikinfrastruktur-Plattform dar. Der Zugriff auf Fachanwendungen der zentralen

Telematikinfrastruktur-Plattform wird für Fachmodule des Konnektors auf gesicherte Fachdienste und für Clientsysteme bzw. Fachmodule im LAN des Leistungserbringers auf offene Fachdienste ermöglicht. Die Kommunikation mit aktiven Bestandsnetzen erfolgt ebenfalls nur über den VPN-Tunnel der zentralen Telematikinfrastruktur-Plattform.

Für den Fall einer Anbindung des lokalen Netzes des Leistungserbringers an das Internet dient der Netzkonnektor als Internet Gateway und stellt einen sicheren Kanal zum Zugangspunkt des sicheren Internet-Dienstleisters sowie einen Paketfilter (IP-Firewall) zur Verfügung.

VPN-Client

Der Netzkonnektor baut mit einem VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform einen VPN-Kanal gemäß dem Standard IPsec (IP Security) auf. Netzkonnektor und VPN-Konzentrator authentisieren sich gegenseitig und leiten einen Sitzungsschlüssel ab, mit dem die Vertraulichkeit und Integrität der nachfolgenden Kommunikation gesichert wird. Dazu nutzt der Netzkonnektor Schlüsselmaterial, welches auf einem dem Netzkonnektor zugeordneten Sicherheitsmodul (gSMC-K) gespeichert ist.

In analoger Weise baut der Netzkonnektor einen VPN-Kanal zum SIS auf. Netzkonnektor und SIS authentisieren sich gegenseitig und leiten einen Sitzungsschlüssel ab, mit dem die Vertraulichkeit und Integrität der nachfolgenden Kommunikation gesichert wird. Dazu nutzt der Netzkonnektor Schlüsselmaterial, welches auf einem dem Netzkonnektor zugeordneten Sicherheitsmodul (gSMC-K) gespeichert ist.

Der VPN-Kanal zum VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform (siehe FTP_ITC.1/NK.VPN_TI für die Kommunikation mit der Telematikinfrastruktur) stellt eine Absicherung der Kommunikationsbeziehung zwischen Netzkonnektor und VPN-Konzentrator auf Netzwerkebene dar. Nach erfolgtem Aufbau des VPN-Tunnels zur Telematikinfrastruktur durch den Netzkonnektor (= EVG) nutzt der Anwendungskonnektor (= IT-Umgebung) diesen Kanal und authentisiert[4] die Organisation des Leistungserbringers gegenüber den Fachdiensten. Dazu nutzt der Anwendungskonnektor Schlüsselmaterial, welches auf einem der Organisation des Leistungserbringers zugeordneten Sicherheitsmodul (SM-B) gespeichert ist.

TLS-Kanal

Die Dienste zum Aufbau von Transport Layer Security (TLS) Kanälen zu verschiedenen Zwecken und Endpunkten werden dem Anwendungskonnektor vom Netzkonnektor zur Verfügung gestellt.

Hierunter fällt beispielsweise der sichere Kanal zwischen Anwendungskonnektor und Fachdiensten, bzw. Zentralen Diensten der TI oder der sichere Kanal zwischen Anwendungskonnektor und Clientsystem im LAN des Leistungserbringers.

Der Anwendungskonnektor ist nicht Teil des EVG. Die über den TLS-Kanal transportierten Daten werden teilweise auf Anwendungsebene weiter geschützt, beispielsweise durch mit einem HBA erstellte Signaturen. Auch diese Funktionalität ist nicht Teil des EVG.

[4] Diese Authentisierung ist nicht Gegenstand des Security Targets.

Anwendungshinweis 1: Siehe Kapitel 1.3.1 des PP [11].

Anwendungshinweis 2: Siehe Kapitel 1.3.1 des PP [11].

1.3.2. Einsatzumgebung des Konnektors

Der Evaluierungsgegenstand ist der Netzkonnektor als Teil des Konnektors. Der EVG umfasst die Software des Netzkonnektors und die Betriebsdokumentation für den Netzkonnektor.

Die Einsatzumgebung des Konnektors als Einbox-Lösung ist in der folgenden Abbildung 2 dargestellt. Insbesondere wird der Netzkonnektor immer mit Konnektorteilen (AK, SM-K bzw. gSMC-K) gemeinsam betrieben, die nach den für diese Konnektorteile anzuwendenden Schutzprofilen, bzw. der Technischen Richtlinie evaluiert und zertifiziert bzw. von der gematik zugelassen wurden.

Anwendungshinweis 3: Dieses ST beschreibt die so genannte „Einbox-Lösung“. Das bedeutet, dass

- Netzkonnektor und Anwendungskonnektor in einer Box integriert sind, und dass
- die gSMC-K sicher mit dem Netzkonnektor verbunden ist, so dass kein weiterer Schutz der Verbindung zwischen Netzkonnektor und gSMC-K erforderlich wird.

Die in Abbildung 2 links vom Transportnetz dargestellten Komponenten befinden sich im lokalen Netz (LAN) des Leistungserbringers und werden als dezentrale Komponenten bezeichnet. Der bzw. die VPN-Konzentratoren und die übrigen rechts bzw. unterhalb vom Transportnetz dargestellten Dienste werden als zentrale Dienste oder zentrale Telematikinfrastruktur-Plattform bezeichnet.

Alle Teilkomponenten des Konnektors sind durch dicke schwarze Rahmen gekennzeichnet. Der Netzkonnektor als ein Teil des Konnektors ist durch blaue Färbung kenntlich gemacht. Der Netzkonnektor stellt den EVG dar – durch die blaue Färbung wird also die physische EVG-Abgrenzung beschrieben. Mit roten Linien werden zum besseren Verständnis Komponenten zusammengefasst, die üblicherweise in einem gemeinsamen Gehäuse untergebracht sind (insbesondere bei der Einbox-Lösung) oder die auf einer gemeinsamen Plattform ablaufen. Abhängig vom Einsatzszenario können die roten Linien geschützten Bereichen (vgl. A.NK.phys_Schutz) entsprechen.

Neben den dargestellten physischen Verbindungen gibt es logische Kanäle, die über die physischen Verbindungen etabliert werden und üblicherweise zusätzlich geschützt werden (sichere Kanäle). Diese Verbindungen sind in der Abbildung 2 aus Gründen der Übersichtlichkeit nicht dargestellt.

Außerdem abstrahiert Abbildung 2 von der Tatsache, dass die SM-B auf verschiedenste Arten an den Anwendungskonnektor angebunden werden kann – etwa mittels eines per LAN angebundenen Kartenterminals.

In der folgenden Abbildung 2 bedeuten die Abkürzungen (siehe auch Kapitel 8.2):

- NK: Netzkonnektor
- AK: Anwendungskonnektor

- EVG: Evaluierungsgegenstand (TOE)
- KT (= eHealth KT): Kartenterminal im Gesundheitswesen; in der folgenden Abbildung ist aus Gründen der Übersichtlichkeit stets nur ein Kartenterminal dargestellt
- PF: LAN-seitiger bzw. WAN-seitiger Paketfilter. Die spitze Seite des Paketfilter-Symbols zeigt jeweils zu der Seite, von der potentielle Angriffe abgewehrt werden sollen.
- Clientsystem-HW: Hardware des Clientsystems. Auf dieser Plattform läuft die Software des Leistungserbringers (z. B. Praxisverwaltungssystem, Apothekenverwaltungs-system, Krankenhaus-Informationssystem).
- PVS: Praxis-Verwaltungssystem. Dieser Ausdruck steht stellvertretend auch für Apotheken-Verwaltungssysteme (AVS) oder Krankenhaus-Informationssysteme (KIS). Er bezeichnet den Softwareanteil auf dem Clientsystem. Das Betriebssystem des Clientsystems ist in den folgenden Abbildungen nicht dargestellt.
- eGK: elektronische Gesundheitskarte
- HBA: Heilberufsausweis
- SM-B: Security Module Card Typ B oder HSM-B, Träger der kryptographischen Identität der Institution des Leistungserbringers
- gSMC-K: Sicherheitsmodul für den Konnektor
- SIS: Sicherer Internet Service
- TI Telematikinfrastruktur-Plattform
- VSDM: Versichertenstammdatenmanagement
- VSDD: Versichertenstammdatendienst

Anwendungshinweis 4: Der WAN-Router ist nicht mit dem Netzkonnektor in einem gemeinsamen Gehäuse integriert.

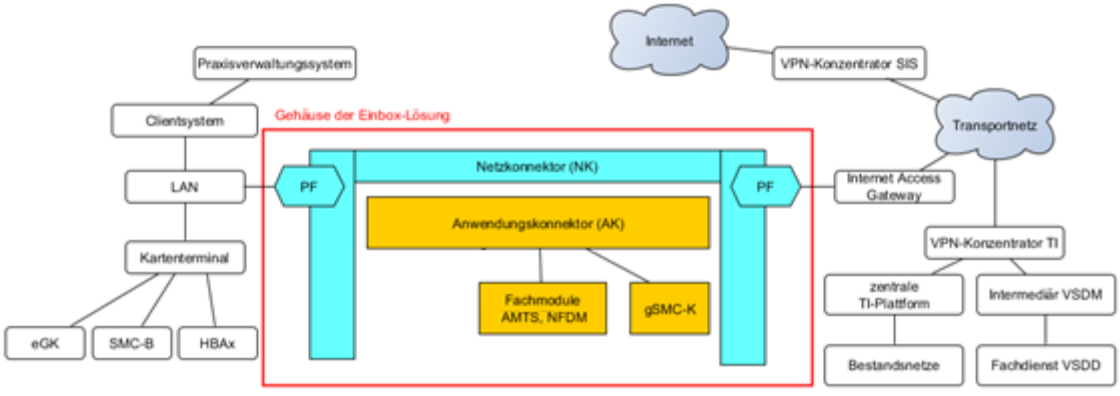

Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung)

Im betrachteten Fall ist der Konnektor als Einbox-Lösung ausgestaltet, hierbei wird der Anwendungskonnektor vom Netzkonnektor durch einen Paketfilter vor Angriffen aus dem LAN geschützt.

Bei der hier als Einbox-Lösung bezeichneten Variante handelt es sich um eine typische Lösung für kleinere und mittlere Arztpraxen oder Apotheken: Netzkonnektor und Anwendungskonnektor laufen in einer gemeinsamen Box ab. Es sind nur geringfügige Eingriffe in die bestehende Infrastruktur erforderlich.

Anwendungshinweis 5: In Abbildung 2 ist die Einsatzumgebung des Netzkonnektors (EVG) beschrieben. Dabei werden die physischen und logischen Schnittstellen zwischen dem EVG und seiner IT-Umgebung skizziert. Eine detailliertere Darstellung der Schnittstellen findet sich in Abschnitt 1.3.3, siehe auch Abbildung 3.

Anwendungshinweis 6: Dieses Security Target modelliert Sicherheitsanforderungen an einen Einbox-Konnektor (Einboxlösung).

Es wird angenommen, dass die Einsatzumgebung des Netzkonnektors diesen vor physischen Angriffen schützt (siehe Annahme A.NK.phys_Schutz in Abschnitt 3.5).

Es wird angenommen, dass die Clientsysteme nicht oder nur in sicherer Weise an potentiell unsichere Netze (z. B. Internet) angebunden sind. Ferner wird angenommen, dass die Clientsysteme nach dem aktuellen Stand der Technik entwickelt wurden und administriert werden, so dass sie das spezifizierte Verhalten zeigen. Für Details siehe Annahme A.NK.Betrieb_**CS** in Abschnitt 3.5.

Anwendungshinweis 7: Außer den benannten Annahmen an die sichere Infrastruktur und Implementierung der Clientsysteme werden keine weiteren Annahmen getroffen.

Anwendungshinweis 8: Spezielle Einsatzumgebungen: Der Netzkonnektor ist für den Betrieb in einer Einsatzumgebung ausgelegt, wie sie im PP [11] definiert wird. Es ergeben sich keine zusätzlichen spezifischen Anforderungen, die über die Vorgaben aus dem PP hinausgehen.

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 9: Der EVG unterstützt alle vom PP BSI-CC-PP-0097-V2-2020-MA-02 erwarteten physischen Schnittstellen und implementiert darüber hinaus die herstellerspezifische Schnittstelle PS5 wie im Folgenden dargestellt.

Der EVG besitzt folgende physische Schnittstellen:

PS1 *Die physische Schnittstelle zum Anwendungskonnektor entfällt aufgrund der Einbox-Lösung.*

PS2 Eine Schnittstelle zum LAN bzw. zum Clientsystem.

Über diese Schnittstelle können Clientsysteme oder andere Systeme im LAN mit dem Konnektor kommunizieren.

PS3 Eine Schnittstelle zu Datennetzen (WAN), welche als Transportnetz für den Zugang zur Telematikinfrastruktur und ggf. zum Internet dienen. Es wird

angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und Verbindungen mit ihnen nicht notwendigerweise verschlüsselt sind.[5]

Anwendungshinweis 10: Durch die für dieses ST relevante Einboxlösung des Konnektors ist die Identifizierung einer physischen Schnittstelle zwischen Netzkonnektor und dem Anwendungskonnektor nicht erforderlich. Die Kommunikation beider Konnektorteile beschränkt sich auf die logische Schnittstelle LS1. In diesem ST wird die Nummerierung aus dem PP BSI-CC-PP-0097-V2-2020-MA-02 beibehalten und PS1 der Vollständigkeit halber aufgeführt. Die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle fallen nicht in einer physischen Schnittstelle zusammen, da getrennte Netzwerkcontroller verwendet werden.

PS4 Eine Schnittstelle zum Sicherheitsmodul des Netzkonnektors (gSMC-K).

Die gSMC-K dient als sicherer Schlüsselspeicher für die **kryptographische Identität** des EVGs (Netzkonnektor) in Form eines privaten Authentisierungsschlüssels und des zugehörigen Zertifikats.

Ein solches Zertifikat ist in eine PKI (Public Key Infrastructure) eingebunden und wird nur für Netzkonnektoren erteilt, die über eine **Bauartzulassung** verfügen. Auf diese Weise wird es den VPN-Konzentratoren der zentralen Telematikinfrastruktur-Plattform ermöglicht, beim Aufbau des VPN-Kanals durch die Netzkonnektoren den Zugriff auf die Telematikinfrastruktur auf bauartzugelassene Netzkonnektoren zu beschränken.

Die gSMC-K ist sicher mit dem EVG verbunden. Siehe auch OE.NK.gSMC-K.

PS5 Eine Schnittstelle zur Signaleinrichtung (Signalisierung).

Der Konnektor verfügt über drei LEDs zur Anzeige von Statusmeldungen (Power, Verbindungsstatus, Fehlerzustand).

Schließlich wird die physische Hülle des Konnektors als weitere Schnittstelle betrachtet. Aufgrund der Annahme A.NK.phys_Schutz werden keine Angriffe über diese Schnittstelle betrachtet. Abbildung 3 zeigt die verfügbaren physischen Schnittstellen des Konnektors sowie deren Zuordnung zu den logischen Schnittstellen. Der Stromanschluss ist keine relevante Schnittstelle im Sinne des zugrundeliegenden PP [11].

Anwendungshinweis 11: Die Schnittstellen sind in Abbildung 2 und Abbildung 3 grafisch dargestellt.

[5] In der Konnektorspezifikation [16] sind Szenarien definiert, die für eine Verbindung zum Transportnetz die Schnittstelle PS2 vorsehen. In diesen Fällen bleibt die Schnittstelle PS3 ungenutzt.

1.3.3.2. Logische Schnittstellen des EVG

Anwendungshinweis 12: Der folgende Abschnitt stellt eine Übersicht über die logischen Schnittstellen des EVG samt ihrer Zuordnung zu den in Kapitel 1.3.3.1 beschriebenen physischen Schnittstellen dar. Alle logischen Schnittstellen aus dem PP [11] sind enthalten. Der EVG implementiert darüber hinaus die herstellerspezifischen Schnittstellen (LS8, LS9) wie im Folgenden dargestellt.

Der EVG besitzt folgende logische Schnittstellen:

LS1 Eine Schnittstelle zum Anwendungskonnektor.

LS2 Eine Schnittstelle zu den Clientsystemen, die physisch über das LAN (PS2) des Leistungserbringers erreichbar sind.

LS3 Eine Schnittstelle zur entfernten Telematikinfrastruktur, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS3)[6] erreicht wird.

LS4 Eine Schnittstelle zum SIS, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS3)[7] erreicht wird.

LS5 Eine Schnittstelle zum ungesicherten Transportnetz, die für den Aufbau der VPN-Kanäle genutzt wird (WAN, via PS3)[8].

LS6 Eine Schnittstelle zu lokalen Managementfunktionen des Netzkonnektors (via PS2).

LS7 Eine Schnittstelle zu einem Sicherheitsmodul für den Netzkonnektor (gSMC-K) (via PS4).

LS8 *entfallen*

LS9 Eine Schnittstelle zur Signaleinrichtung (Signalisierung) zur Statusanzeige. Über diese Schnittstelle werden die LEDs zur Anzeige des Verbindungsstatus und zur Anzeige von Fehlerzuständen (kritische Betriebszustände) gemäß Konnektor-Spezifikation [16], Abschnitt 3.3 (via PS5) angesteuert.

Anwendungshinweis 13: Der EVG bietet keine Schnittstelle für entferntes Management an.

[6] In der Konnektorspezifikation [16] sind Szenarien definiert, die für eine Verbindung zum Transportnetz die Schnittstelle PS2 vorsehen. In diesen Fällen bleibt die Schnittstelle PS3 ungenutzt.

[7] In der Konnektorspezifikation [16] sind Szenarien definiert, die für eine Verbindung zum Transportnetz die Schnittstelle PS2 vorsehen. In diesen Fällen bleibt die Schnittstelle PS3 ungenutzt.

[8] In der Konnektorspezifikation [16] sind Szenarien definiert, die für eine Verbindung zum Transportnetz die Schnittstelle PS2 vorsehen. In diesen Fällen bleibt die Schnittstelle PS3 ungenutzt.

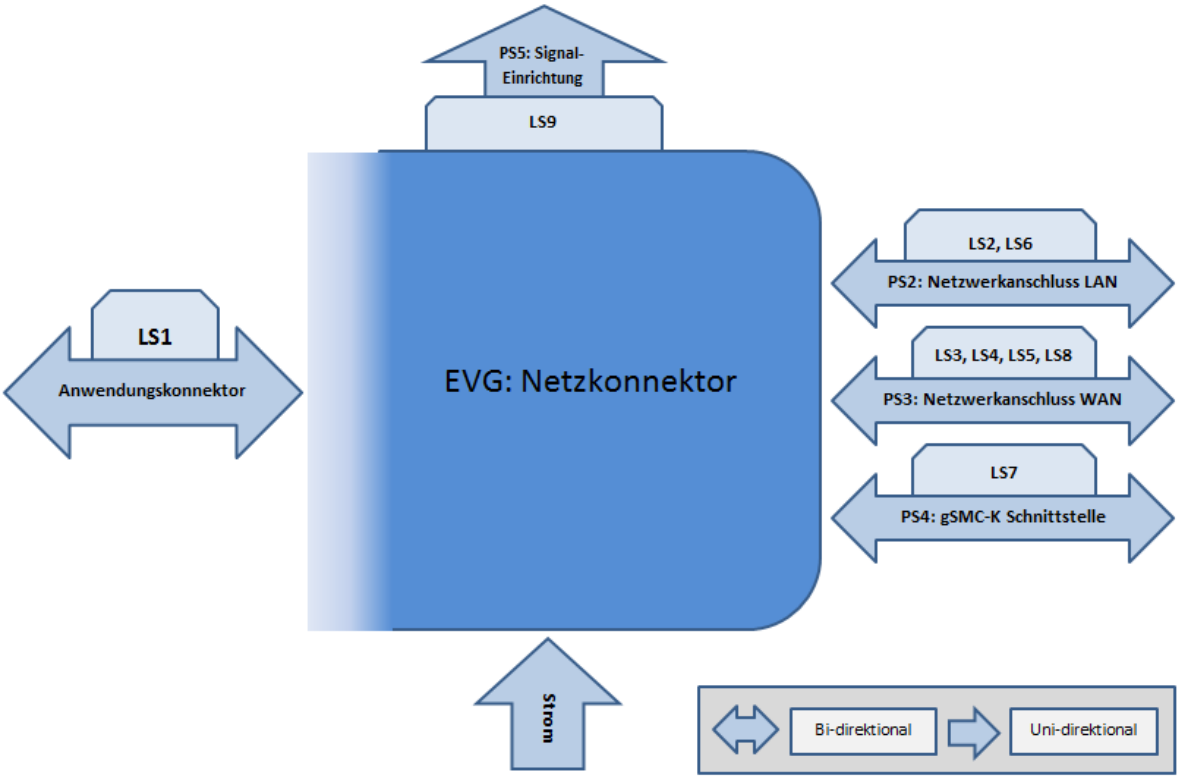

Abbildung 3: Konnektor: externe, physische und logische Schnittstellen

1.3.4. Aufbau und physische Abgrenzung des Netzkonnektors

Zur Gesamtarchitektur und für einen Überblick über die Kernkonzepte sei auf die Konnektor-Spezifikation [16] verwiesen. Eine grobe Abgrenzung des Netzkonnektors von den übrigen Teilen des Konnektors erfolgte bereits in Abschnitt 1.3.

Anwendungshinweis 14: Die Abbildung 4 stellt das allgemeine Architekturkonzept des gesamten Konnektors dar. Hieraus wird die Einordnung des EVG ersichtlich.

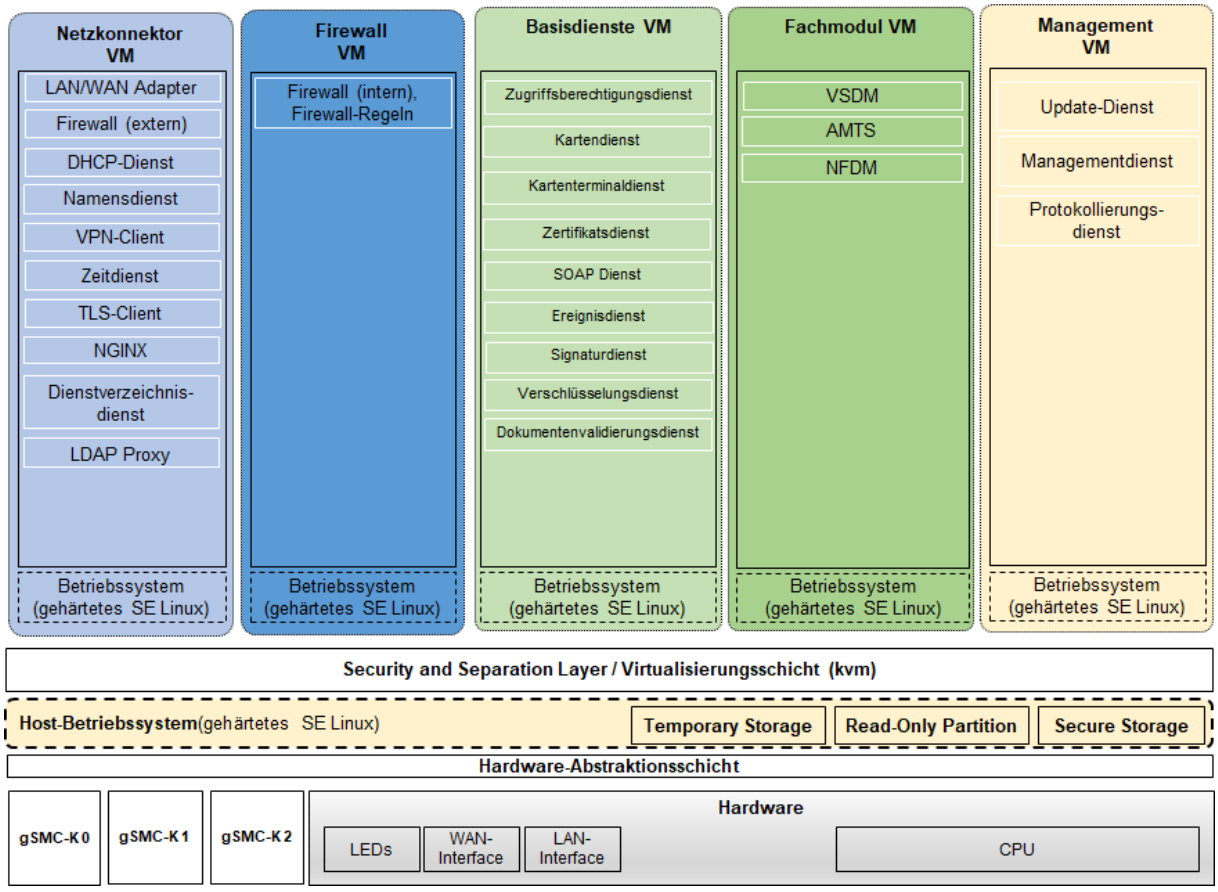

Abbildung 4:: Konnektor Architekturkonzept (schematisch)

Architekturübersicht

Der in diesem Security Target definierte Evaluierungsgegenstand umfasst die Software des Netzkonnektors und die Betriebsdokumentation für den Netzkonnektor. Die Hardware des Konnektors ist nicht Teil des EVGs, diese ist in Kapitel 1.3.6 genauer beschrieben. In Abbildung 4 wird die gesamte Architektur des Konnektors inklusive Hardware und Softwareanteile des Anwendungskonnektors dargestellt.

Die Software für den Betrieb eines Konnektors wird modular aufgebaut, wobei jedem Modul eine dezidierte Aufgabe übertragen wird und dieses jeweils unabhängig und unbeeinflusst von anderen Modulen betrieben wird.

Als Grundlage für die Umsetzung des Konnektors wird ein gehärtetes Linux-System eingesetzt, welches als Betriebssystem unter anderem für die Verwaltung der Hardwareressourcen (z.B. CPU Scheduling, Arbeitsspeicherverwaltung) verantwortlich zeichnet. Das Linux-System wurde genau an die Sicherheits- und Anwendungsanforderungen des Konnektors angepasst.

Der HAL (Hardware Abstraction Layer) ist integraler Bestandteil des Kernels und wird mit Hilfe von Linux Gerätetreibern umgesetzt; beispielsweise kommt für die Kommunikation mit der gSMC-K ein entsprechender Linux-Treiber zum Einsatz. Damit ist es Anwendungen möglich, mit einer Gerätekarte mittels APDUs (Application Protocol Data Unit) auf sicherem Wege zu kommunizieren.

Aufbauend auf dem HAL und dem Betriebssystem werden einzelne Module – wie beispielsweise Fachmodule oder das Management-Modul – primär mittels Java und C/C++ implementiert und jeweils in eigenständigen Anwendungscontainern betrieben. Die Module sind in entsprechend ihrer Funktionalität gruppiert und in verschiedene virtuelle Umgebungen eingebunden. Somit sind nicht nur die betriebenen Module, sondern auch die gemeinsamen Betriebssystem-Komponenten logisch separiert. Dazu wird ein Virtualisierungs-Hypervisor eingesetzt welcher als Teil des Linux-Host-Betriebssystems installiert und betrieben wird.

Im Folgenden werden die einzelnen Funktionsblöcke des Konnektors beschrieben, in denen als virtuelle Umgebungen (Virtual Machine, VM) einzelne Module zusammengefasst sind:

- **Netzkonnektor VM:** Diese VM übernimmt die Aufgabe der Sicherung von Netzwerkkommunikation im lokalen Netzwerk (z.B. Kommunikation mit angeschlossenen Kartenterminals) sowie mit der TI-Plattform. Dies umfasst beispielsweise Implementierung von lokalen Netzwerkdiensten (z.B. DNS), Firewall und die TLS und VPN-Anbindung an die TI-Plattform, für welche auch Routing-Funktionalität bereitgestellt wird und somit die Transportsicherung der TI-Plattform sichergestellt wird.

- **Firewall VM:** Diese VM überwacht die Kommunikation der einzelnen Module untereinander. Dabei handelt es sich nicht um die nach außen angebotene Firewall-Funktionalität des Netzkonnektors. Diese wird in der Netzkonnektor VM implementiert. Die Firewall VM als zentraler Dienst übernimmt auch Protokollierungsaufgaben.

- **Basisdienste VM:** Die Basisdienste VM setzt die Funktionalität des Anwendungskonnektors um. Der Basiskonnektor übernimmt auch die Aufgabe der Kommunikation mit den Gerätekarten (über den Treiber), und ist die einzige VM, die über die Treiber-API auf die Gerätekarten zugreifen darf. Sicherheitsaufgaben wie Verschlüsselung oder Signaturerstellung bzw. -prüfung sind ebenfalls durch den Basiskonnektor abgebildet.

- **Fachmodule VM:** Durch die beschriebene Architektur wird ein flexibler Einsatz von mehreren unterschiedlichen Fachmodulen ermöglicht. Solche können im Rahmen eines Firmware-Updates über das „Management-Modul“ installiert und verwaltet werden.

- **Management VM:** Implementiert das Management-Interface für lokale und entfernte Administration. Damit wird einem Benutzer die Möglichkeit zur Verwaltung des Konnektors gegeben. Unter anderem wird durch diese VM die Zertifikats- und Userverwaltung abgebildet.

  Diese VM übernimmt auch die Aufgabe, alle anderen Module über vorgesehene Schnittstellen zu konfigurieren, sodass sämtliche Systemparameter (inkl. anderer Module, Betriebssystem) in dieser VM abgebildet werden können. Damit wird eine einzelne und zentrale Stelle zur Systemkonfiguration des Konnektors geschaffen.

  Zusätzlich kann ein autorisierter Benutzer über das Management-Interface Informationen zum Systemstatus (z.B. Betriebsstatus der einzelnen Module) abrufen. Des Weiteren wird der Firmware-Upgrade Prozess in dieser VM abgebildet. Eine neue

Firmware-Version kann nur nach bestandener Integritäts- und Authentizitätsprüfung sowie bestandener Versionsprüfungen installiert werden.

Ausschließlich die Management VM hat die Möglichkeit signierte Firmware-Updates einzuspielen.

Die EVG Bestandteile sind

- Netzkonnektor VM
- Firewall VM
- Zertifikatsdienst und Kartendienst (Module der Basisdienste VM)
- Management VM

Alle benannten Teile des Konnektor befinden sich wie in Abbildung 2 angezeigt innerhalb eines Gehäuses. Die physische Abgrenzung des Netzkonnektors ist durch die „Einbox-Lösung“ des Konnektors definiert.

1.3.5. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste

Der EVG erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [16] definierten Schnittstellen weitgehend automatisch. Der EVG ermöglicht ein Management (Administration) nach Autorisierung des Administrators. Die Autorisierung des Administrators erfolgt sowohl für den Netzkonnektor als auch für den Anwendungskonnektor durch das Management Modul (Abschnitt 1.3.4, Management VM). Dieses Modul wird in diesem Security Target dem Netzkonnektor zugeordnet. Die Authentisierung des Administrators erfolgt daher durch den EVG selbst.

Anwendungshinweis 15: Authentisierung des Administrators: Das Mangement Modul implementiert einen gemeinsamen Administrator-Account für Netzkonnektor und Anwendungskonnektor. Die Authentisierung des Konnektor-Administrators wird formal dem NK zugeordnet. Der Anwendungskonnektor (AK) übernimmt den Authentisierungszustand. Aufgrund der Annahme A.NK.phys_Schutz ist dabei keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) erforderlich. Da der EVG die Authentisierung des Administrators selbst durchführt; wurde das Umgebungsziel OE.NK.Admin_Auth aus dem PP [11] in ein EVG-Ziel O.NK.Admin_Auth umgewandelt.

Anwendungshinweis 16: Vollständigkeit der Dienste: Die Dienste wurden aus dem Netzkonnektor PP [11] übernommen. Es wurden keine zusätzlichen Dienste modelliert.

Anwendungshinweis 17: Der Netzkonnektor gewährleistet keine Transaktionssicherheit. Soweit Transaktionssicherheit aus Sicherheitsgründen erforderlich ist, wird sie im Clientsystem und/oder in der zentralen Telematikinfrastruktur-Plattform hergestellt.

Der EVG erbringt die folgenden Sicherheitsdienste gemäß PP BSI-CC-PP-0097-V2-2020-MA-02:

VPN-Client: Der EVG stellt einen sicheren Kanal (virtual private network, VPN) zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) zwecks Nutzung von Diensten bereit. Der sichere Kanal zur TI wird zur Kommunikation zwischen Anwendungskonnektor und Fachdiensten, Netzkonnektor und zentralen Diensten sowie zwischen Clientsystemen und Bestandsnetzen genutzt. Ferner stellt der EVG einen sicheren Kanal (VPN) zum SIS her. Dieser Kanal dient der Verbindung der lokalen Netzwerke der Leistungserbringer mit dem Internet.

(a) Der EVG erzwingt die Authentisierung des Kommunikationspartners (VPN-Konzentrator und SIS) und ermöglicht eine Authentisierung gegenüber diesen Partnern; diese erfolgt auf der Basis von Standard IPsec und mit Hilfe von Zertifikaten nach dem Standard X.509v3. Siehe auch Sicherheitsdienst Gültigkeitsprüfung von Zertifikaten.

Der Netzkonnektor authentisiert sich gegenüber den genannten Kommunikationspartnern mittels Schlüsselmaterial, das sich auf einem Sicherheitsmodul gSMC-K befindet.

(b) Die Nutzdaten, die über das VPN übertragen werden, werden hinsichtlich ihrer Vertraulichkeit und Datenintegrität geschützt (Verschlüsselung und Integritätsschutz der Daten vor dem Versenden bzw. der Entschlüsselung und der Integritätsprüfung nach dem Empfangen). Dazu wird für die VPN-Verbindung ein Sitzungsschlüssel vereinbart.

Der Netzkonnektor muss die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen erzwingen und ungeschützten Zugriff auf das Transportnetz verbieten. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[9], aber er muss ihre versehentliche Preisgabe verhindern.

Dynamischer Paketfilter: Der EVG bindet die Clientsysteme sicher an die Telematikinfrastruktur, den SIS und die Bestandsnetze (über die TI) an. Dazu verfügt der EVG über die Funktionalität eines dynamischen Paketfilters, welcher entsprechende Regeln umsetzen kann. Der EVG schützt das lokale Netz des Leistungserbringers vor Angriffen aus dem Transportnetz und sich selbst vor Angriffen aus dem Transportnetz und dem lokalen Netz des Leistungserbringers. Hierbei werden Angriffe mit hohem Angriffspotential abgewehrt. Der EVG beschränkt den freien Zugang zu dem und von dem als unsicher angesehenen Transportnetz. Die Inhalte der Kommunikation zur Telematikinfrastruktur werden von Netzkonnektor nicht ausgewertet. In jedem Fall unterbindet der Netzkonnektor direkte Kommunikation (außerhalb von VPN-Kanälen) ins Transportnetz (WAN, Internet) mit Ausnahme der für den VPN-Verbindungsaufbau erforderlichen Kommunikation[10] sowie Verbindungen zum CRL Download Server.

[9] Beispielsweise könnte ein HBA-Inhaber zu schützende Daten der TI und der Bestandsnetze von einem Clientsystem aus lokal auf Wechseldatenträger kopieren.

[10] Das betrifft insbesondere DNS-Anfragen zur Auflösung der Adresse des VPN Konzentrators sowie Protokolle zum Aufbau des VPN-Tunnels (IKEv2)

Anwendungshinweis 18: Der LAN-seitiger Paketfilter hindert Schadsoftware, die möglicherweise auf anderen Wegen (z. B. Wechseldatenträger wie CD, DVD, USB-Stick, Diskette) in die IT-Systeme im LAN des Leistungserbringers gelangt, daran die Integrität des Konnektors zu bedrohen.

Anwendungshinweis 19: Der Netzkonnektor enthält kein Application Layer Gateway in dem Sinne, dass der Anwendungskonnektor auf einem eigenen Layer implementiert wird. Vielmehr ist der Gesamtkonnektor modular aufgebaut. Die einzelnen Module laufen auf einem Security and Separation Layer (Virtualisierungsschicht), siehe auch Abschnitt 1.3.4. Aus Sicht des Gesamtkonnektors wird zudem der Anwendungskonnektor topologisch von beiden Seiten von einem Paketfilter umgeben (LAN-seitig und WAN-seitig, d.h. gegenüber dem Clientsystemnetz und gegenüber dem Transportnetz; siehe auch Abbildung 2).

TLS-Basisdienst: Der EVG stellt Basisdienste für den Aufbau von TLS-Kanälen zur Verfügung und ermöglicht eine Authentisierung der Kommunikationspartner. Siehe auch Sicherheitsdienst Gültigkeitsprüfung von Zertifikaten

Anwendungshinweis 20: Hinweis: Die Entscheidung, für welche Verbindungen diese TLS-Kanäle genutzt werden, liegt beim Anwendungskonnektor, also außerhalb des EVG.

Der EVG bietet folgende netzbasierte Dienste an:

Zeitdienst: Der Netzkonnektor stellt einen NTP-Server der Stratum-3-Ebene für Fachmodule und Clientsysteme bereit, welcher die Zeitangaben eines NTP Servers Stratum-2-Ebene der zentralen Telematikinfrastruktur-Plattform in regelmäßigen Abständen abfragt. Der EVG kann die synchronisierte Zeit anderen Komponenten des Konnektors zur Verfügung stellen. Die vom EVG bereitgestellte Zeit-Information wird für die Prüfung der Gültigkeit von Zertifikaten genutzt, und um die Audit-Daten des Sicherheits-Logs mit einem Zeitstempel zu versehen.

Anwendungshinweis 21: Durch den Netzkonnektor erfolgt eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK. Die Konnektor-Spezifikation [16] sieht vor, dass die Zeitsynchronisation ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform erfolgt, d.h. über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur.

DHCP-Dienst: Der EVG stellt an der LAN-Schnittstelle (PS2) die Funktion eines DHCP Servers gemäß RFC 2131 [37] und RFC 2132 [38] zur Verfügung.

DNS-Dienst: Der EVG stellt an der LAN-Schnittstelle (PS2) und an der Schnittstelle zum AK (PS1) die Funktion eines DNS-Servers zur Verfügung.

Gültigkeitsprüfung von Zertifikaten: Der EVG muss die Gültigkeit der Zertifikate des Kommunikationspartners überprüfen, die für den Aufbau eines VPN-Kanals oder TLS-Kanals verwendet werden.[11] Zu diesem Zweck wird eine TSL (Trust-Service Status List) verteilt, welche Zertifikate von Diensteanbietern enthält, die Gerätezertifikate ausstellen können. Der EVG kann anhand der aktuell gültigen TSL die Gültigkeit der Gerätezertifikate seiner Kommunikationspartner prüfen. Ferner wird eine zugehörige CRL (Certificate Revocation

[11] Die Überprüfung des Zertifikats des EVG erfolgt durch den Kommunikationspartner. Eine Überprüfung der eigenen, für den Aufbau eines VPN Kanal verwendeten Zertifikate durch den EVG ist nicht erforderlich.

List) bereitgestellt, die der EVG ebenfalls auswertet. Außerdem überprüft der EVG, dass die verwendeten Algorithmen gültig sind. Siehe auch Sicherheitsdienst VPN-Client ((a): Authentisierung der Kommunikationspartner).

Anwendungshinweis 22: Die Prüfung der Algorithmen erfolgt implizit durch den EVG, indem sichergestellt wird (im Rahmen der Evaluierung), dass der EVG nur gültige Algorithmen verwendet. Die Verwendung ungültig gewordener Algorithmen wird dadurch verhindert wird, dass – unter Verwendung des Software-Update-Mechanismus des EVGs bzw. des Gesamtkonnektors – ein Update eingespielt wird.

Stateful Packet Inspection: Der EVG kann nicht-wohlgeformte IP-Pakete erkennen und implementiert eine zustandsgesteuerte Filterung (stateful packet inspection).

Anwendungshinweis 23: Der Konnektor realisiert kein netzwerkbasiertes Intrusion Detection System (IDS) für das Clientsystemnetz.

Darüber hinaus implementiert der EVG folgende übergeordnete Dienste:

Selbstschutz: Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren. Der EVG schützt Geheimnisse (insbesondere Schlüssel) während ihrer Verarbeitung gegen unbefugte Kenntnisnahme.

Speicheraufbereitung: Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben.

Selbsttests: Der EVG bietet seinen Benutzern eine Möglichkeit, die Integrität des EVGs zu überprüfen.

Protokollierung: Der EVG führt ein Sicherheits-Log (security log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher muss hinreichend groß dimensioniert sein. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [16].

Anwendungshinweis 24: Die Auswertung des Sicherheits-Logs erfolgt durch die Einsatzumgebung. Es werden vom Netzkonnektor keine Auswertungen durchgeführt, die über die Anforderungen der Konnektor-Spezifikation [16] hinausgehen.

Anwendungshinweis 25: Die geschützte Speicherung des Protokolls (u. a. zyklisches Überschreiben, Schutz gegen Manipulation durch den Administrator) wird als übergreifende Funktionalität im PP [12] gefordert (siehe dort, FAU_STG.1/AK und FAU_STG.4/AK).

Administration: Der EVG bietet eine lokale Managementschnittstelle an. Die Managementschnittstelle wird durch das Management Modul vom Netzkonnektor ungesetzt.

Anwendungshinweis 26:

An der Managementschnittstelle werden Wartungsaktivitäten, wie die Verwaltung von Clientsystemen, Verwaltung von LAN/WAN Anbindungen inkl. Einstellungen bzgl. VPN, Konfiguration von Diensten (Kartendienst, Zertifikatsdienst, Kartenterminaldienst, Systeminformationsdienst, Protokollierungsdienst, Zeitdienst, Signaturdienst) und Fachmodulen (VSDM), Einstellungen bezüglich DHCP und DNS, Management des Informationsmodelles und des allegeminen Betriebes, Konfiguration zum KSR Client. Verwaltung von Registrierungsinformationen und Benutzerverwaltung.

Eine Möglichkeit zur Fernwartung (remote Management) ist nicht implementiert.

Der EVG erzwingt eine sichere **Authentisierung des Administrators** vor administrativen Aktivitäten. Die Authentisierung wird durch den Netzkonnektor selbst durchgeführt. Die Zugriffskontrolle (nur authentisierte Administratoren dürfen administrative Tätigkeiten und Wartungsarbeiten durchführen) ist ebenfalls Sicherheitsfunktionalität des Netzkonnektors.

1.3.6. Non-EVG Hardware/Software/Firmware

Der EVG umfasst die Software des Netzkonnektors. Dabei wird der Netzkonnektor immer mit den Konnektorteilen Anwendungskonnektor und der Security Module Card Konnektor gSMC-K gemeinsam betrieben, siehe auch die Beschreibung zur Einsatzumgebung in Kapitel 1.3.2. Als Hardware wird der Versionsstand *1.0.0* verwendet.

Der Netzkonnektor bietet dabei dem Anwendungskonnektor eine sichere Plattform und stellt die in diesem Security Target definierten Sicherheitsfunktionen zur Verfügung. Dazu nutzt der EVG die Sicherheitsfunktion der gSMC-K. Das Betriebssystem der gSMC-K und das Objektsystem der gSMC-K muss durch die gematik zugelassen worden sein.

Anwendungshinweis 27: Der Netzkonnektor wird als reine Software-Lösung implementiert. Die Hardware ist nicht Teil des EVGs.

Die Hardware des Einbox-Konnektors ist in einem vollständig geschlossenen Gehäuse mit externem Netzteil. Das Gehäuse besitzt die in Kapitel 1.3.3.1 beschriebenen physischen Schnittstellen, insbesondere Netzwerkports für WAN und LAN Verbindungen, USB-Ports und LEDs für die Signaleinrichtung. Im Gehäuse sind drei gSMC-Ks des Konnektors verbaut. Als gSMC-Ks werden durch die gematik zugelassene STARCOS 3.6 Health SMCK R1 (BSI-K-TR-0253-2016) für Generation 2 bzw. STARCOS 3.7 gSMC-K R1, Version 1.0.2 für Generation 2.1 verwendet. In der folgenden Tabelle sind die Mindestanforderungen an die HW Komponenten der Einbox-Konnektor Hardware beschrieben:

Komponente	**Beschreibung**
CPU	x86-64
RAM	8GB
Harddisk	16GB
Netzwerk	Zwei getrennte Netzwerkcontroller für LAN (PS2) und WAN (PS3)

Smartcard-Leser (für gSMC-K)	3x interne CCID kompatible USB Leser oder Onboard-Kartenleser für ID-000 Karten (SIM-Kartenformat)
RTC	Real-Time-Clock mit einem definierten Drift von maximal +/- 20ppm

Tabelle 3: Mindestanforderungen für Komponenten der Einbox-Konnektor Hardware

2. Postulat der Übereinstimmung

2.1. Common Criteria Konformität

Das Security Target wurde gemäß Common Criteria Version 3.1 Revision 5 erstellt:

[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

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

und unter Berücksichtigung von

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

Es wurde eine funktionale Sicherheitsanforderung (FPT_EMS.1/NK, siehe Abschnitt 5.1.) definiert, die nicht in CC Teil 2 [2] enthalten ist. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [3] entnommen.

Daher ist dieses Security Target:

CC Teil 2 [2] erweitert (extended) und

CC Teil 3 [3] konform (conformant).

2.2. Security Target-Konformität

Dieses Security Target behauptet „**strict conformance**“ Konformität zum

Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097-V2-2020-MA-02, [11].

2.3. Paket-Konformität

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponente

- AVA_VAN.5 (Resistenz gegen Angriffspotential „hoch“),

- ADV_FSP.4 (Vollständige Funktionale Spezifikation),
- ADV_TDS.3 (Einfaches Modulares Design),
- ADV_IMP.1 (TSF-Implementierung),
- ALC_TAT.1 (Wohldefinierte Entwicklungswerkzeuge) und
- ALC_FLR.2 (Verfahren für Problemreports).

In diesem Security Target werden die vom Schutzprofil BSI-CC-PP-0097-V2-2020-MA-02 geforderten Vertrauenswürdigkeitsanforderungen übernommen.

2.4. Begründung der Konformität

Das Security Target verwendet funktionale Sicherheitsanforderungen aus CC Teil 2 [2] sowie eine funktionale Sicherheitsanforderung, die nicht in CC Teil 2 [2] enthalten ist, daher ist das Security Target CC Teil 2 erweitert (extended).

Das Security Target verwendet nur Anforderungen an die Vertrauenswürdigkeit aus CC Teil 3 [3], daher ist das Security Target CC Teil 3 konform (conformant).

Das Security Target übernimmt die Definition des EVG-Typs sowie des Sicherheitsproblems, der Sicherheitsziele und der Sicherheitsanforderungen aus dem zugrundeliegenden Protection Profile BSI-CC-PP-0097-V2-2020-MA-02. Da das Security Target keine Konformität zu weiteren Schutzprofilen behauptet, können auch keine Widersprüche zwischen diesem Security Target und weiteren Schutzprofilen im EVG-Typ oder in der Definition des Sicherheitsproblems, der Sicherheitsziele und der Sicherheitsanforderungen auftreten.

Das zugrundeliegende Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, wie sie in CC Teil 3 [3] definiert ist, zusammen mit der Komponente AVA_VAN.5, um Schutz gegen hohes Angriffspotenzial zu erreichen. Durch direkte und indirekte Abhängigkeiten der Komponente AVA_VAN.5 müssen die Komponenten ADV_IMP.1 und ALC_TAT.1 neu aufgenommen werden und die Komponenten ADV_TDS.3 und ADV_FSP.4 augmentiert werden. Darüber hinaus wurde die Stufe EAL3 noch um die Komponente ALC_FLR.2 augmentiert, die keine Abhängigkeiten besitzt; für die Gründe dazu siehe Abschnitt 6.6. Das Security Target übernimmt die Vertrauenswürdigkeitsstufe des Schutzprofils. Damit sind alle Anforderungen an die Konformität erfüllt.

3. Definition des Sicherheitsproblems

In diesem Abschnitt wird zunächst beschrieben, welche Werte (Assets) durch den EVG geschützt werden, welche externen Einheiten mit ihm interagieren und welche Objekte von Bedeutung sind. Auf dieser Basis wird danach beschrieben, welche Bedrohungen der EVG abwehren muss, welche organisatorischen Sicherheitspolitiken zu beachten sind und welche Annahmen an seine Einsatzumgebung getroffen werden können.

Bedrohungen, organisatorischen Sicherheitspolitiken sowie Annahmen wurden entsprechend zum zugrundeliegenden PP mit dem zusätzlichen Kürzel „NK“ versehen. Damit wird die Herkunft dieser Artefakte eindeutig mit „Netzkonnektor“ gekennzeichnet.

3.1. Zu schützende Werte

Werte (Assets) sind die durch Gegenmaßnahmen zu schützenden Informationen oder Ressourcen des EVGs. Der Schutz kann durch den EVG selbst oder durch die Umgebung erfolgen; diese Aufteilung erfolgt in Kapitel 4.

Zu schützende Daten

Der Begriff „zu schützende Daten der TI und der Bestandsnetze“ bezeichnet im Folgenden stets medizinische oder sonstige personenbezogene Daten (einschließlich Daten des Versicherten), die aus dem Zuständigkeitsbereich des Leistungserbringers in die Verantwortung der Telematikinfrastruktur bzw. in die Bestandsnetze übergehen, und umgekehrt. Diese Daten sind *User Data* im Sinne der Common Criteria. Sie umfassen bei den Pflichtanwendungen nach § 291 a SGB V [9] mindestens die Versichertenstammdaten[12] und elektronische Verordnungen (eVerordnungen) sowie sonstige Daten, die im Rahmen der Abwicklung dieser Pflichtanwendungen entstehen (etwa Dispensierdaten).

Bei den zu schützenden Werten wird zwischen primären und sekundären Werten unterschieden:

> Primäre Werte sind die ursprünglichen Werte, die auch vor Einführung des EVG bereits existierten. Ein typisches Beispiel für einen primären Wert sind Klartext-Nutzdaten, deren Vertraulichkeit zu schützen ist.
>
> Sekundäre Werte sind solche Werte, die durch die Einführung des EVG erst entstehen, durch diesen bedingt werden oder von den primären Werte abgeleitet werden können. Ein typisches Beispiel für einen sekundären Wert sind Schlüssel; etwa solche, die zum Schutz der Vertraulichkeit der Nutzdaten verwendet werden.

[12] Man beachte, dass aus dem Zuzahlungsstatus der Versichertenstammdaten Rückschlüsse über den Empfang von Sozialleistungen (Arbeitslosigkeit) oder über bestehende chronische Krankheiten (Erreichen der Zuzahlungsgrenze) gezogen werden können.

3.1.1. Primäre Werte

Die primären Werte sind in der folgenden Tabelle 4 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler Telematikinfra-struktur-Plattform (beide Übertragungs-richtungen)	Vertraulichkeit, Integrität, Authentizität	Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform werden zu schützende Daten der TI und der Bestandsnetze ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein. ⇒ T.NK.local_EVG_LAN, T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_VPN_Data, A.NK.AK, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.Zert_Prüf, T.NK.DNS
zu schützende Nutzerdaten während der Übertragung zwischen Konnektor und sicherem Internet Service	Vertraulichkeit, Integrität, Authentizität	Beim Zugriff auf Internet-Dienste werden Nutzerdaten zwischen den lokalen Netzen der Leistungserbringer und dem sicheren Zugangspunkt zum Internet ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der angegebene Schutz der Authentizität bezieht sich auf die Tunnel-Endpunkte, nicht auf die im Tunnel übertragenen Daten. ⇒ T.NK.local_EVG_LAN, T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_VPN_Data, A.NK.AK, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.Zert_Prüf, T.NK.DNS
zu schützende Daten der TI und der Bestandsnetze im Clientsystem	Vertraulichkeit, Integrität	Auf den Clientsystemen werden zu schützende Daten der TI und der Bestandsnetze vorgehalten. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten manipulieren können. ⇒ T.NK.remote_EVG_LAN, A.NK.phys_Schutz
in der zentralen Telematikinfrastruktur-Plattform oder auf Chip-karten gespeicherte zu schützende Daten der TI und der Bestandsnetze	Vertraulichkeit, Integrität	Werden zu schützende Daten der TI und der Bestandsnetze in der zentralen Telematikinfrastruktur-Plattform gespeichert, so dürfen diese, abhängig von ihrem Schutzbedarf (abhängig vom Fachdienst), auch dort nicht unbefugt eingesehen oder unbemerkt verändert werden können. ⇒ T.NK.remote_VPN_Data, A.NK.sichere_TI
Clientsystem, Anwendungskonnektor	Integrität	Manipulierte Clientsysteme oder Anwendungskonnektoren können dazu führen, dass zu schützende Daten der TI und der Bestandsnetze abfließen oder unautorisiert verändert werden. Im normalen Betrieb wird davon ausgegangen, dass zu schützende Daten der TI und der Bestandsnetze das Clientsystem nur dann verlassen, wenn sie in die zentrale Telematikinfrastruktur-Plattform oder auf eine eGK übertragen werden sollen. Daher werden zu schützende Daten der TI und der Bestandsnetze nur durch den Anwendungskonnektor bzw. (im Fall von Daten der Bestandsnetze) den Netzkonnektor übermittelt. Ein manipuliertes Clientsystem könnte Kopien der Daten einem Angreifer

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		zugänglich machen oder auch zu schützende Daten der TI und der Bestandsnetze gezielt verändern. Ein manipulierter Anwendungskonnektor (oder Fachmodule) könnte zu schützende Daten der TI und der Bestandsnetze falsch übergeben und so die korrekte Übermittlung durch den Netzkonnektor (über den VPN-Kanal zur Telematikinfrastruktur) verhindern. Auf diese Weise könnte einem Versicherten oder einem Leistungserbringer Schaden zugefügt werden. ⇒ T.NK.remote_EVG_LAN, A.NK.Betrieb_AK, A.NK.Betrieb_CS, A.NK.phys_Schutz
Systeme der zentralen Telematikinfrastruktur-Plattform	Verfügbarkeit	Der Anwendungskonnektor kann Syntaxprüfungen und Plausibilisierungen von Anfragen an die zentrale Telematikinfrastruktur-Plattform durchführen und auf diese Weise dazu beitragen, dass weniger nicht wohlgeformte Anfragen an die zentrale Telematikinfrastruktur-Plattform gerichtet werden. Bei diesen Aspekten handelt es sich aber um Bedrohungen der zentralen Telematikinfrastruktur-Plattform und nicht um Bedrohungen des EVG. Außerdem kann der Konnektor nicht für die Verfügbarkeit von Diensten garantieren; daher wird Verfügbarkeit nicht als Sicherheitsziel für den EVG formuliert. ⇒ A.NK.kein_DoS, A.NK.Ersatzverfahren

Tabelle 4: Primäre Werte

Die primären Werte, deren zu schützenden Eigenschaften und das daraus abgeleitete Bedrohungspotential bzw. erforderliche Annahmen entsprechen Tabelle 1 des zugrundeliegenden PPs [11]

3.1.2. Sekundäre Werte

Die sekundären Werte sind in der folgenden Tabelle 5 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze im EVG	Vertraulichkeit, Integrität	Auch während der Verarbeitung im EVG müssen zu schützende Daten der TI und der Bestandsnetze gegen unbefugte Kenntnisnahme und Veränderung geschützt werden. ⇒ T.NK.local_EVG_LAN T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN
kryptographisches Schlüsselmaterial (während seiner Speicherung im EVG oder Verwendung durch den EVG)	Vertraulichkeit, Integrität, Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikationspartners sicherzustellen.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		⇒ A.NK.phys_Schutz, T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.Zert_Prüf
Authentisierungs-geheimnisse (im EVG gespeicherte Referenzdaten und zum EVG übertragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungsgeheimnissen (z. B. Passwort für Administratorauthentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit)
Management-Daten (während ihrer Übertragung zum EVG)	Vertraulichkeit, Integrität und Authentizität	Wenn der EVG administriert wird, dürfen die administrativen Datenströme nicht eingesehen oder unbemerkt verändert werden können. ⇒ T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit Das gilt auch für die im Rahmen der Laufzeitverlängerung erneuerten gSMC-K-Zertifikate des EVGs.
Management-Daten (während ihrer Speicherung im EVG)	Integrität	Management-Daten (z. B. Konfigurationsdaten) des EVG dürfen nicht unbemerkt verändert werden können, da sonst nicht mehr sichergestellt ist, dass der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit) Das gilt auch für die im Rahmen der Laufzeitverlängerung erneuerten gSMC-K-Zertifikate des EVGs.
Sicherheits-Log-Daten (Audit-Daten)	Integrität, Verfügbarkeit	Der EVG muss Sicherheits-Log-Daten generieren, anhand derer Veränderungen an der Konfiguration des EVG nachvollzogen werden können (vgl. O.NK.Protokoll und FAU_GEN.1/NK.SecLog). Niemand darf Sicherheits-Log-Daten löschen oder verändern können. Wenn der für die Sicherheits-Log-Daten vorgesehene Speicherbereich aufgebraucht ist, können die Sicherheits-Log-Daten zyklisch überschrieben werden. Die Sicherheits-Log-Daten müssen auch zum Nachweis der Aktivitäten von Administratoren verwendet werden können. ⇒ T.NK.remote_EVG_WAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit
Systemzeit	Verfügbarkeit, Gültigkeit	Der EVG muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern synchronisieren. Die Zeit wird für die Prüfung der Gültigkeit von VPN-Zertifikaten sowie für die

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		Erzeugung von Zeitstempeln in Sicherheits-Log-Daten oder Audit-Daten verwendet. ⇒ T.NK.TimeSync

Tabelle 5: Sekundäre Werte

Die sekundären Werte, deren zu schützenden Eigenschaften und das daraus abgeleitete Bedrohungspotential bzw. erforderliche Annahmen entsprechen Tabelle 2 des zugrundeliegenden PPs [11].

3.2. Externe Einheiten, Subjekte und Objekte

Die Formulierung des Sicherheitsproblems (Security Problem Definition) erfolgt unter Verwendung der im Folgenden beschriebenen externen Einheiten (*external entities*). Mit dem Begriff *external entity* werden gemäß den Definitionen[13] in Common Criteria v3.1R5 [1] Einheiten außerhalb des EVGs bezeichnet, mit denen der EVG interagieren kann. Eine solche *external entity* kann der EVG intern als Subjekt abbilden – ob er dies tut, hängt davon ab, ob er die externe Einheit identifizieren kann.

3.2.1. Externe Einheiten (*external entities*)

In der Einsatzumgebung des EVGs gibt es folgende externe Einheiten:

AK Anwendungskonnektor, entspricht S_AK des BSI-CC-PP-0098-V3-2021-MA-03

VPN-TI entfernter VPN-Konzentrator, der den Zugriff auf die Telematikinfrastruktur vermittelt,

VPN-SIS entfernter VPN-Konzentrator, der den sicheren Zugriff auf das Internet realisiert,

DNS-ext (externer) DNS-Server für den Namensraum Internet

Zeit-ext (externer) Zeit-Server des Zugangsnetzproviders

CS Clientsystem,

TSL/CRL Bereitstellungspunkte für TSL und CRL

[13] Definitionen in Common Criteria [1], Kapitel 3: ***subject*** *:= an active entity in the EVG that performs operations on objects;* ***object*** *:= a passive entity in the EVG, that contains or receives information, and upon which subjects perform operations;* ***external entity*** *:= any entity (human or IT) outside the EVG that interacts (or may interact) with the EVG.*

NK-Admin oder auch **NK-Administrator**: Administrator des Netzkonnektors, fällt zusammen mit S_Administrator des BSI-CC-PP-0098-V3-2021-MA-03.

S_KSR „Update-Server“ in der TI. Stellt freigegebene Firmware-Update-Pakete für den TOE und eHealth Kartenterminals zum Download bereit.

Angreifer ein Angreifer.

Der **NK-Admin** authentisiert sich gegenüber dem Konnektor (siehe O.NK.Admin_EVG).

Der **Angreifer** kann sich sowohl gegenüber dem Netzkonnektor als (gefälschter) VPN-Konzentrator als auch gegenüber einem VPN-Konzentrator als (gefälschter) Netzkonnektor ausgeben.

Ersteres wird durch die Bedrohungen T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.remote_VPN_Data und T.NK.remote_admin_WAN (für den VPN-Tunnel in die Telematikinfrastruktur) abgebildet. Es wird nicht ausgeschlossen, dass auch ein Versicherter oder ein Leistungserbringer als Angreifer auftreten können:

Der **Versicherte** hat keinen direkten Zugriff auf den Konnektor, deshalb wird er hier nicht gesondert modelliert. Außerdem ist er natürlich am Schutz der Werte (Nutzdaten, z. B. medizinische Daten) interessiert. Insofern werden über den Schutz der Werte die Interessen des Versicherten berücksichtigt. Ein Versicherter kann in der Rolle des Angreifers auftreten.

Für den **Leistungserbringer** sind die Leistungen des NK transparent, er arbeitet mit dem Clientsystem. Sofern er Einstellungen des NK verändert, agiert er in der Rolle des NK-Administrators. Deshalb sind Leistungserbringer bzw. HBA-Inhaber nicht gesondert als eigene externe Einheiten modelliert. Auch ein Leistungserbringer könnte grundsätzlich in der Rolle des Angreifers auftreten: Innerhalb des NK gibt es Geheimnisse (z. B. Sitzungsschlüssel des VPN-Kanals), die auch ein Leistungserbringer nicht kennen soll. Versucht ein Leistungserbringer, Kenntnis von diesen Geheimnissen zu erlangen, kann dies als Angriff betrachtet werden. Beim Leistungserbringer gilt jedoch folgende Einschränkung: Weder der NK noch der Anwendungskonnektor können gegen den Willen eines Leistungserbringers Datenschutzanforderungen durchsetzen, solange Clientsysteme dies nicht unterstützen. Daher werden solche potentiellen Angriffe eines Leistungserbringers hier **nicht** betrachtet (das Verhindern solcher Angriffe ist nicht Bestandteil der EVG-Sicherheitspolitik). Im Umfeld des Konnektors wird der Leistungserbringer als vertrauenswürdig angesehen, da er üblicherweise auch die Erfüllung des Umgebungsziels OE.NK.phys_Schutz sicherstellen muss.

3.2.2. Objekte

Es werden die folgenden Objekte betrachtet:

CS-Daten lokal beim Leistungserbringer (in Clientsystemen im LAN) gespeicherte zu schützende Daten der TI und der Bestandsnetze,

VPN-Daten-TI zu schützende Daten der TI und der Bestandsnetze während des Transports zwischen NK und VPN-K der Telematikinfrastruktur,

VPN-Daten-SIS *zu schützende Nutzerdaten* während des Transports zwischen NK und VPN-SIS

TI-Daten entfernt in den Datenbanken der Telematikinfrastruktur bzw. den Bestandsnetzen gespeicherte zu schützende Daten der TI und der Bestandsnetze.

Update-Pakete Software-Komponenten eines zukünftigen EVG, die im Sinne eines Update Prozesses zur Aktualisierung der laufenden Version der Software-Komponente des EVG dienen soll.

O_LZV_Zert_gSMCK im Rahmen der Laufzeitverlängerung erneuerte gSMC-K-Zertifikate des EVGs (EVG-Identitäten der gSMC-K):

- C.SAK.AUT
- C.NK.VPN
- C.AK.AUT
- C.SAK.AUTD_CVC

Der jeweilige Zertifikatstyp (RSA und/oder ECC) der vom TSP zur Verfügung gestellten Zertifikate hängt dabei von den auf der gSMC-K vorhandenen Zertifikaten ab.

Es wird davon ausgegangen, dass die VPN-Daten durch den zwischen NK und VPN-Konzentratoren implementierten sicheren Kanal (d.h. durch das VPN) geschützt werden und dass die TI-Daten nur in verschlüsselter Form gespeichert vorliegen (z. B. eVerordnung) (siehe A.NK.sichere_TI in Abschnitt 3.5). Die Sicherheit der Clientsysteme ist nicht Gegenstand der Betrachtung.

3.3. Bedrohungen

3.3.1. Auswahl der betrachteten Bedrohungen

Eine Motivation der in Abschnitt 3.3.2 beschriebenen Bedrohungen sowie eine Beschreibung der möglichen Angriffspfade ist dem PP [11], Abschnitt 3.3.1 zu entnehmen und wird in diesem Security Target nicht wiederholt. Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen werden wie folgt zusammengefasst:

- Angriffe aus dem Transportnetz gegen IT-Komponenten des Leistungserbringers oder auch gegen den Netzkonnektor selbst (mit Ziel CS-Daten, siehe T.NK.remote_EVG_WAN und T.NK.remote_EVG_LAN),
- Angriffe aus dem Transportnetz auf die Datenübertragung zwischen dem lokalen Netz des Leistungserbringers und der zentralen Telematikinfrastruktur-Plattform (mit Ziel VPN-Daten-TI, siehe T.NK.remote_VPN_Data); hier sind die Vertraulichkeit und Integrität der übertragenen Daten sowie die Authentizität von Sender und Empfänger bedroht.

- Angriffe aus dem Transportnetz auf die Datenübertragung zwischen dem lokalen Netz des Leistungserbringers und dem Sicheren Internet Service (mit Ziel VPN-Daten-SIS anzugreifen, siehe T.NK.remote_VPN_Data); hier sind die Vertraulichkeit und Integrität der übertragenen Daten bedroht.
- Lokale Angriffe auf die Integrität des Netzkonnektors (siehe T.NK.local_EVG_LAN) mit dem Ziel, dessen Sicherheitseigenschaften zu schwächen oder zu verändern.
- Zudem erlaubt der EVG lokale und entfernte Administration, die ebenfalls das Ziel von Angriffen sein können (siehe T.NK.local_admin_LAN und T.NK.remote_admin_WAN).

3.3.2. Liste der Bedrohungen

Die folgende Abbildung 5 zeigt die beschriebenen externen Einheiten, Objekte und Angriffspfade (nummerierte Pfeile) im Zusammenhang.

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt. Das Kästchen „LAN-Interface“ stellt entweder die Verbindung zum Anwendungskonnektor dar oder schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

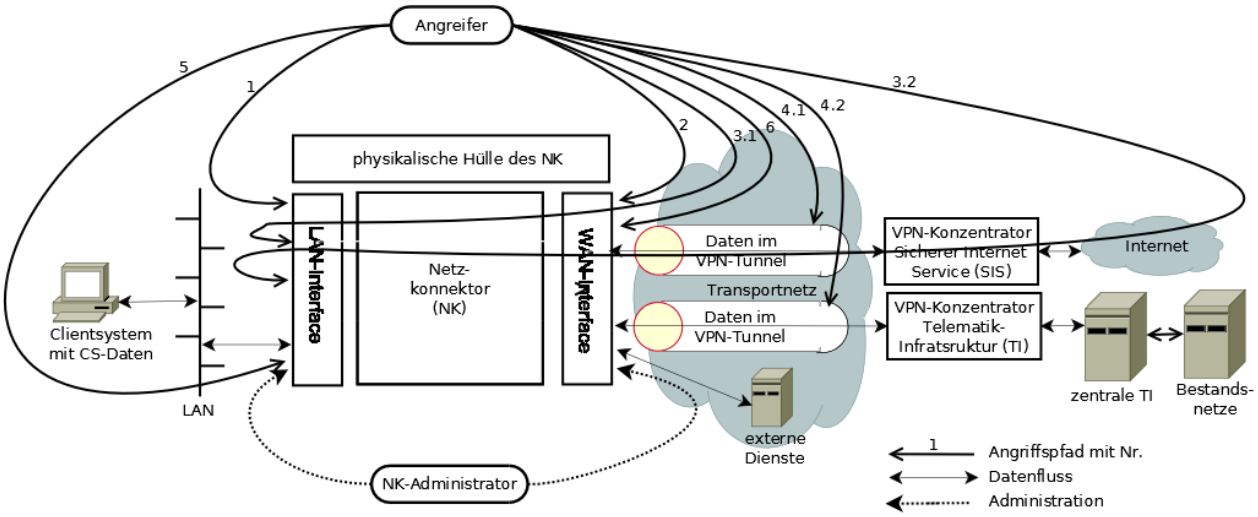

Abbildung 5: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 5 visualisierten Angriffspfaden (Nr. 1 bis Nr. 6) bzw. den zugeordneten Bedrohungen könnte ein Angreifer

- unbemerkt ganze Konnektoren durch Nachbauten ersetzen (T.NK.counterfeit) oder
- die Kommunikation mit netzbasierten Diensten (Bezug von Sperrlisten für Gültigkeitsprüfung von Zertifikaten, Zeitsynchronisation, DNS) manipulieren (T.NK.Zert_Prüf, T.NK.TimeSync, T.NK.DNS).

Die Bedrohungen werden im restlichen Dokument mit den folgenden Bezeichnern referenziert:

Angriffspfad	Bezeichner	Beschreibung in Abschnitt
Nr. 1	T.NK.local_EVG_LAN	3.3.2.1
Nr. 2	T.NK.remote_EVG_WAN	3.3.2.2
Nr. 3.1	T.NK.remote_EVG_LAN	3.3.2.3
Nr. 3.2	T.NK.remote_EVG_LAN	3.3.2.3
Nr. 4.1	T.NK.remote_VPN_Data	3.3.2.4
Nr. 4.2	T.NK.remote_VPN_Data	3.3.2.4
Nr. 5	T.NK.local_admin_LAN	3.3.2.5
Nr. 6	T.NK.remote_admin_WAN	3.3.2.6
Konnektornachbauten	T.NK.counterfeit	3.3.2.7
Zertifikatsstatusabfragen	T.NK.Zert_Prüf	3.3.2.8
Zeitsynchronisation	T.NK.TimeSync	3.3.2.9
DNS-Manipulation	T.NK.DNS	3.3.2.10

Tabelle 6: Kurzbezeichner der Bedrohungen

In den folgenden Abschnitten werden die Bedrohungen genauer beschrieben.

Die Angriffe, deren Bezeichner das Wort „local“ enthalten (T.NK.local_EVG_LAN und T.NK.local_admin_LAN) nehmen an, dass der Angreifer lokal in den Räumlichkeiten des Leistungserbringers agiert, setzen also einen unbefugten physischen Zugriff auf den Netzkonnektor (z. B. Einbruch) voraus. Dabei wird angenommen, dass Personen, die berechtigten Zugang zu vor physischen Zugriff geschützten Bereichen des Leistungserbringers haben, entweder vertrauenswürdig[14] sind (so dass von ihnen keine Bedrohungen ausgehen, z. B. Arzt selbst, Servicetechniker, einige Angestellte) oder dass der physische Zugriff durch den Leistungserbringer geeignet beschränkt wird (z. B. Patienten dürfen zwar Wartezimmer und Behandlungsräume betreten, aber nicht auf den gesicherten Bereich zugreifen in welchem der Konnektor aufbewahrt wird – siehe die Annahme A.NK.phys_Schutz).

Die Angriffe, deren Bezeichner das Wort „remote“ enthalten (T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.remote_VPN_Data und T.NK.remote_admin_WAN), nehmen an, dass der Angreifer über keinen solchen physischen Zugriff auf Geräte erlangt, sondern dass die Angriffe ausschließlich über das Transportnetz (z. B. Internet) erfolgen.

Die Angriffe, deren Bezeichner das Wort „admin“ enthalten (T.NK.local_admin_LAN und T.NK.remote_admin_WAN), nehmen an, dass ein Angreifer die

[14] genauer: vertrauenswürdig im Umfeld des Netzkonnektors bzw. im Rahmen der Bedrohungen, die der Netzkonnektor abwehren kann; Angriffe auf das Gesamtsystem werden hier nicht betrachtet.

Administrationsschnittstelle(n) des Netzkonnektors ausnutzt, um unbefugt Sicherheitseinstellungen zu verändern oder zu deaktivieren.

3.3.2.1. T.NK.local_EVG_LAN

Ein Angreifer dringt lokal in die Räumlichkeiten des Leistungserbringers ein und greift den Netzkonnektor über dessen LAN-Schnittstelle an. Der Angreifer verfügt über hohes Angriffspotential.[15] Ziel bzw. Motivation des Angriffs ist es, den Netzkonnektor zu kompromittieren, um

- den Netzkonnektor zu kompromittieren, um im Netzkonnektor gespeichertes kryptographisches Schlüsselmaterial, Management-Daten, Authentisierungsgeheimnisse und zu schützende Daten der TI und der Bestandsnetze im Netzkonnektor in Erfahrung zu bringen,
- den Netzkonnektor so zu manipulieren, dass zukünftig vertrauliche zu schützende Daten der TI und der Bestandsnetze und zu schützende Nutzerdaten während der Übertragung kompromittiert werden können, oder
- den Netzkonnektor so zu manipulieren, dass zukünftig zu schützende Daten der TI und der Bestandsnetze und zu schützende Nutzerdaten während der Übertragung unbemerkt manipuliert werden können.

Für diesen Angriff kann der Angreifer sowohl vorhandene IT-Systeme im LAN des Leistungserbringers nutzen als auch eigene (z. B. Notebook, Netbook, PDA[16], Smartphone/Handy) mitbringen.

Nicht vom Anwendungskonnektor generierter direkter Verkehr aus dem LAN könnte an die Telematikinfrastrukturdienste für Dienste gemäß § 291 a SGB V gelenkt werden.

Einen Spezialfall dieses Angriffs stellt das Szenario dar, dass ein IT-System im LAN durch lokale Kontamination mit bösartigem Code verseucht wird und danach Angriffe gegen den Netzkonnektor an dessen LAN-seitiger Schnittstelle vornimmt. Lokale Kontamination bedeutet dabei, dass ein lokaler Angreifer den bösartigen Code direkt auf das IT-System im LAN aufbringt, beispielsweise durch Wechseldatenträger (CD, USB-Stick, etc.).

Ebenfalls betrachtet werden Angriffe, bei denen ein Angreifer den Netzkonnektor durch manipulierte Aufrufe aus dem Clientsystem-Netz in einen unsicheren Systemzustand zu bringen versucht.

---

[15] Aufgrund der Vielzahl möglicher Angreifer soll hier bewusst keine nähere Spezifikation des Angreifers vorgenommen werden. Das hohe Angriffspotential impliziert (siehe CEM [4], Anhang A.8.2 *Calculating attack potential*), Aussagen über die Expertise und die Ressourcen für Angriffe. Denkbar sind für alle in diesem Security Target aufgeführten Bedrohungen sowohl Angriffe einzelner Personen (z.B. Beziehungstaten, Rache) als auch organisierte Angriffe. Auch das Ziel der Angriffe kann in einem breiten Spektrum variieren zwischen dem Wunsch, gezielt Daten über einzelne Opfer auszuspähen (Ex-Partner, Prominente(r), Politiker(in), etc.) und dem Wunsch, die großen Mengen vertraulicher Daten in der zentralen Telematikinfrastruktur in vielerlei Hinsicht auszuwerten.

[16] Personal Digital Assistant

Anwendungshinweis 28: Der EVG verfügt über einen LAN-seitigen Paketfilter, der den Netzkonnektor vor potentiellen Angriffen aus dem LAN schützt. Der LAN-seitige Paketfilter des Netzkonnektors schützt in der vorliegenden Einbox-Lösung auch den Anwendungskonnektor.

3.3.2.2. T.NK.remote_EVG_WAN

Ein Angreifer greift den Konnektor aus dem Transportnetz heraus an. Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer nutzt Fehler des Netzkonnektors aus, um den Konnektor zu kompromittieren – mit allen Aspekten wie in Abschnitt 3.3.2.1 T.NK.local_EVG_LAN beschrieben. Der Angreifer greift den Netzkonnektor unbemerkt über das Netzwerk an, um unautorisierten Zugriff auf weitere Werte zu erhalten.

3.3.2.3. T.NK.remote_EVG_LAN

Ein Angreifer greift den Konnektor aus dem Transportnetz bzw. Internet heraus an. Der Angreifer verfügt über hohes Angriffspotential. Ziel ist wieder eine Kompromittierung des Konnektors, mit allen Aspekten wie bereits in Abschnitt 3.3.2.1 T.NK.local_EVG_LAN beschrieben. Im Gegensatz zur Bedrohung T.NK.remote_EVG_WAN ist das Ziel jedoch nicht, den Netzkonnektor direkt an seiner WAN-Schnittstelle anzugreifen, sondern über den Netzkonnektor zunächst Zugriff auf das lokale Netz des Leistungserbringers (LAN) zu erhalten, um dort ein Clientsystem zu kompromittieren und möglicherweise im Anschluss daran den Konnektor von dessen LAN-Seite her anzugreifen. Die Kompromittierung eines Clientsystems ist gegeben, wenn ein Angreifer aus dem Transportnetz bzw. dem Internet unautorisiert auf personenbezogene Daten im Clientsystem zugreifen kann oder wenn der Angreifer ein Clientsystem erfolgreich und unbemerkt manipulieren kann.

Hierzu werden in Abbildung 5 zwei Angriffspfade unterschieden:

Im Fall von Angriffspfad 3.1 nutzt der Angreifer Fehler des Netzkonnektors aus, um die vom Netzkonnektor als Sicherheitsfunktion erbrachte Trennung der Netze (Transportnetz / LAN) zu überwinden. Bereits eine Überwindung dieser Trennung stellt einen erfolgreichen Angriff dar. Wird darüber hinaus in der Folge über die LAN-Schnittstelle des Konnektors unerwünschtes Verhalten herbeigeführt, so stellt dies eine erfolgreiche Fortführung des Angriffs dar.

Im Fall von Angriffspfad 3.2 nutzt der Angreifer Fehler in der Sicherheitsfunktion des Sicheren Internet Service aus, um über den VPN-Tunnel Zugriff auf IT-Systeme im LAN zu erlangen. Dabei kann auch der Netzkonnektor über dessen LAN Interface angegriffen werden.

Einen Spezialfall dieses Angriffs (Angriffspfad 3.1 oder 3.2) stellt das Szenario dar, dass ein IT-System im LAN vom Transportnetz bzw. Internet (WAN) aus mit bösartigem Code verseucht wird und in der Folge Angriffe gegen den Konnektor an dessen LAN-seitiger Schnittstelle vornimmt. Ein IT-System im LAN könnte vom Transportnetz aus mit bösartigem

Code verseucht werden, wenn der Netzkonnektor keine effektive Netztrennung[17] zwischen WAN und LAN leistet.

Betroffene zu schützende Werte sind:

- zu schützende Daten der TI und der Bestandsnetze während der Übertragung
- zu schützende Nutzerdaten während der Übertragung
- zu schützende Daten der TI und der Bestandsnetze im Clientsystem
- Clientsystem, Anwendungskonnektor
- zu schützende Daten der TI und der Bestandsnetze im Netzkonnektor
- kryptographisches Schlüsselmaterial
- Authentisierungsgeheimnisse
- Management-Daten (während ihrer Speicherung im Netzkonnektor)
- Sicherheits-Log-Daten

Anwendungshinweis 29: Der EVG verfügt über einen LAN-seitigen Paketfilter, der den Netzkonnektor vor potentiellen Angriffen aus dem LAN schützt. Der LAN-seitige Paketfilter des Netzkonnektors schützt in der vorliegenden Einbox-Lösung auch den Anwendungskonnektor.

3.3.2.4. T.NK.remote_VPN_Data

Ein Angreifer aus dem Transportnetz hört Daten ab oder manipuliert Daten unbemerkt, die zwischen dem Konnektor und der zentralen Telematikinfrastruktur-Plattform (Angriffspfad 4.2 aus Abbildung 5) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 5) übertragen werden. Der Angreifer verfügt über hohes Angriffspotential.

Dies umfasst folgende Aspekte:

- Ein Angreifer gibt sich dem Netzkonnektor gegenüber als VPN-Konzentrator aus (evtl. auch man-in-the-middle-Angriff), um unautorisierten Zugriff auf vom Clientsystem übertragene Daten zu erhalten.
- Ein Angreifer verändert verschlüsselte Daten während der Übertragung unbemerkt.

Betroffene zu schützende Werte sind:

- zu schützende Daten der TI und der Bestandsnetze während der Übertragung
- zu schützende Nutzerdaten während der Übertragung
- in der zentralen Telematikinfrastruktur-Plattform gespeicherte Daten

[17] Das setzt ein entsprechendes Einsatzszenario des Konnektors voraus, bei dem die Kommunikation zum Internet über den Netzkonnektor erfolgt.

3.3.2.5. T.NK.local_admin_LAN

Ein Angreifer dringt lokal in die Räumlichkeiten des Leistungserbringers ein und verändert (im Rahmen lokaler Administration) sicherheitsrelevante Einstellungen des Netzkonnektors. Dies kann dem Angreifer einerseits dadurch gelingen, dass der Netzkonnektor das Verändern von sicherheitsrelevanten Einstellungen nicht hinreichend schützt (im Sinne einer Zugriffskontrolle), oder andererseits dadurch, dass sich ein Angreifer erfolgreich als Administrator ausgeben und mit dessen Berechtigungen agieren kann (im Sinne einer Authentisierung/Autorisierung). Der Angreifer verfügt über hohes Angriffspotential. Ziel des Angreifers kann es sein, Sicherheitsfunktionen des Netzkonnektors zu deaktivieren (z. B. Abschalten der Verschlüsselung auf dem VPN-Kanal oder Erlauben bzw. Erzwingen kurzer Schlüssellängen), die Integrität des Netzkonnektors selbst zu verletzen, Schlüssel auszulesen, um damit Zugriff auf geschützte Daten zu erhalten oder auch die Grundlagen für weiteren Missbrauch zu legen – etwa durch Einspielen schadhafter Software, welche Kopien aller vom Netzkonnektor übertragenen Daten am VPN-Tunnel vorbei zum Angreifer spiegelt.

Diese Bedrohung umfasst auch folgende Aspekte:

- Ein lokaler Angreifer bringt schadhafte Software auf den Netzkonnektor auf.
- Ein lokaler Angreifer greift unautorisiert auf genutzte kryptographische Schlüssel im Arbeitsspeicher des Netzkonnektors zu.
- Ein lokaler Angreifer deaktiviert die Protokollierungsfunktion des Netzkonnektors.
- Ein lokaler Angreifer spielt ein Backup eines anderen Konnektors ein und überschreibt damit Daten (etwa Konfigurationsdaten).
- Ein lokaler Angreifer kann mit modifizierten Konfigurationsdaten beispielsweise per dynamischem Routing den Netzwerkverkehr umleiten.

3.3.2.6. T.NK.remote_admin_WAN

Ein Angreifer verändert aus dem Transportnetz heraus sicherheitsrelevante Einstellungen des Netzkonnektors (im Rahmen zentraler Administration[18]). Dies kann dem Angreifer einerseits dadurch gelingen, dass der Netzkonnektor das Verändern von sicherheitsrelevanten Einstellungen nicht hinreichend schützt bzw. an seiner WAN-Schnittstelle verfügbar macht (im Sinne einer Zugriffskontrolle), oder andererseits dadurch, dass sich ein Angreifer erfolgreich als Administrator ausgeben und mit dessen Berechtigungen agieren kann (im Sinne einer Authentisierung/Autorisierung). Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer verfolgt dieselben Ziele wie unter T.NK.local_admin_LAN besprochen.

Diese Bedrohung umfasst auch folgende Aspekte:

- Ein Angreifer aus dem Transportnetz bringt schadhafte Software auf den Netzkonnektor auf.

[18] Der vorliegende EVG unterstützt die Remote Administration nicht. Diese Bedrohung verbleibt wegen strikter Konformität zum unterliegenden PP in diesen Sicherheitsvorgaben.

- Ein Angreifer aus dem Transportnetz greift unautorisiert auf genutzte kryptographische Schlüssel im Arbeitsspeicher des Netzkonnektors zu.
- Ein Angreifer aus dem Transportnetz deaktiviert die Protokollierungsfunktion des Netzkonnektors.

3.3.2.7. T.NK.counterfeit

Ein Angreifer bringt gefälschte Netzkonnektoren in Umlauf, ohne dass dies vom VPN-Konzentrator erkannt wird[19]. Der Angriff kann durch den unbemerkten Austausch eines bereits im Einsatz befindlichen Geräts erfolgen – wozu in der Regel ein Eindringen in die Räumlichkeiten des Leistungserbringers erforderlich ist – oder bei der Erstauslieferung durchgeführt werden. Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer verfolgt dieselben Ziele wie unter T.NK.local_admin_LAN besprochen.

3.3.2.8. T.NK.Zert_Prüf

Ein Angreifer manipuliert Sperrlisten, die im Rahmen der Gültigkeitsprüfung von Zertifikaten zwischen dem EVG und einem netzbasierten Dienst (siehe OE.NK.PKI) ausgetauscht werden (Wert: zu schützende Daten der TI bei der Übertragung), um mit einem inzwischen gesperrten Zertifikat unautorisierten Zugriff auf Systeme und Daten zu erhalten. Ein bereits gesperrtes Zertifikat wird dem EVG gegenüber als noch gültig ausgegeben, indem eine veraltete oder manipulierte Sperrliste verteilt wird. Dazu kann der Angreifer Nachrichten des Sperrlisten-Verteilungspunkts manipulieren oder sich selbst als dieser Verteilungspunkt ausgeben.

3.3.2.9. T.NK.TimeSync

Ein Angreifer manipuliert Nachrichten, die im Rahmen der Zeitsynchronisation zwischen dem EVG und einem netzbasierten Dienst (Zeitdienst) ausgetauscht werden, oder gibt sich selbst als Zeitdienst aus, um auf dem EVG die Einstellung einer falschen Systemzeit zu bewirken. Der Angreifer verfügt über hohes Angriffspotential.

3.3.2.10. T.NK.DNS

Ein Angreifer manipuliert aus dem Transportnetz heraus Antworten auf DNS-Anfragen zu externen DNS-Servern. Dies kann einerseits Anfragen des Netzkonnektors betreffen, wenn dieser vor dem Aufbau von VPN-Kanälen die Adresse des VPN-Konzentrators der TI oder des SIS ermitteln will. Im Ergebnis wird keine oder eine falsche Adresse ausgeliefert, so dass der Netzkonnektor ggf. die VPN-Verbindung zu einem gefälschten Endpunkt aufbaut, der beispielsweise eine gefälschte zentrale TI-Plattform vorspiegelt. Dadurch werden die zu schützenden Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur-Plattform bedroht. Andererseits können gefälschte DNS-Antworten auch beim Internet-Zugriff von Clientsystemen der

[19] Der Netzkonnektor kann seinen eigenen Diebstahl oder das In-Umlauf-Bringen gefälschter Geräte nicht verhindern; die Authentizität des Netzkonnektors muss letztlich der VPN-Konzentrator sicherstellen. Der Netzkonnektor kann aber zum Erkennen solcher Angriffe beitragen, indem er sich gegenüber dem VPN-Konzentrator authentisiert. Daher zielt die Bedrohung T.NK.counterfeit auf das unbemerkte Fälschen bzw. Austauschen von Netzkonnektoren.

Leistungserbringer auftreten. In einem solchen Szenario könnte der Angreifer den Zugriff der Clientsysteme auf manipulierte Systeme umleiten (Wert: zu schützende Nutzerdaten während der Übertragung zwischen Konnektor und sicherem Internet Service), um Clientsysteme mit bösartigem Code zu infizieren, der dann das lokale Netz, den Netzkonnektor und die zu schützenden Werte bedroht.

3.4. Organisatorische Sicherheitspolitiken

OSP.NK.Zeitdienst Zeitdienst

Der EVG stellt einen Zeitdienst bereit. Dazu führt er in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch.

OSP.NK.SIS Sicherer Internet Service

Die Einsatzumgebung des EVG stellt einen gesicherten Zugangspunkt zum Internet bereit. Dieser Zugangspunkt schützt die dahinter liegenden Netze der Benutzer wirksam gegen Angriffe aus dem Internet. Von diesem Zugangspunkt gehen keine Angriffe auf die angeschlossenen LANs aus.

OSP.NK.BOF Kommunikation mit Bestandsnetzen und offenen Fachdiensten

Der EVG ermöglicht den aktiven Komponenten im LAN des LE eine Kommunikation mit den Bestandsnetzen und den offenen Fachdiensten über den VPN-Kanal zur TI.

OSP.NK.TLS TLS-Kanäle mit sicheren kryptographische Algorithmen

Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [18]. Zudem prüft der EVG die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

OSP.NK.SW-Update Software-Update

Die Software von Konnektorkomponenten kann aktualisiert werden (Software-Update) und zusätzliche Fachmodule können nachgeladen werden. Dabei ist die (ggf. automatische) Auslieferung des Updates bzw. Fachmoduls durch das Konfigurations- und Software Repository (KSR, Update-Server) über einen sicheren Kanal an den Leistungserbringer und die (ggf. automatische) Installation des Updates bzw. Fachmoduls durch den Administrator zu unterscheiden.

Es dürfen nur von einer autorisierten Stelle geprüfte, freigegebene und ggf. zertifizierte Komponenten bzw. Fachmodule zum Update bereit gestellt werden. Die Updates können automatisch installiert werden, wenn dies explizit vom Administrator so konfiguriert wurde.

Bevor ein Software-Update installiert wird, wird die Integrität und Authentizität / Zulässigkeit der Software überprüft (Signaturprüfung und Prüfung der Identität des Signierenden, Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen). Schlägt die Prüfung der Integrität fehl, verhindert der EVG eine Aktualisierung der Software. Falls das Aktivieren einer neuen Software-Version fehlschlägt, wird der letzte funktionierende Software-Stand der Komponente reaktiviert.

Hinweis: OSP.NK.SW-Update wurde von OSP.SW-Update aus dem Protection Profile BSI-CC-PP-0098-V3-2021-MA-03 [12] abgeleitet.

3.5. Annahmen

A.NK.phys_Schutz Physischer Schutz des EVG („sichere Umgebung“)

Die Sicherheitsmaßnahmen in der Umgebung schützen den Konnektor (während aktiver Datenverarbeitung im Konnektor) vor physischem Zugriff Unbefugter. Befugt sind dabei nur durch den Betreiber des Konnektors namentlich autorisierte Personen (z. B. Leistungserbringer, ggf. medizinisches Personal). Sowohl während als auch außerhalb aktiver Datenverarbeitung im Konnektor stellen die Sicherheitsmaßnahmen in der Umgebung sicher, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass die einzuleitenden materiellen, organisatorischen und/oder personellen Maßnahmen größeren Schaden abwehren.

A.NK.gSMC-K Sicherheitsmodul für den EVG (gSMC-K)

Der EVG hat Zugriff auf ein Sicherheitsmodul (gSMC-K), das sicher mit dem EVG verbunden ist. Sicher bedeutet in diesem Fall, dass die gSMC-K nicht unbemerkt vom EVG getrennt werden kann und dass die Kommunikation zwischen gSMC-K und EVG weder mitgelesen noch manipuliert werden kann.

Die gSMC-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des EVG repräsentiert und welches auch für O.NK.VPN_Auth verwendet wird. Es führt kryptographische Operationen mit diesem Schlüsselmaterial durch (Authentisierung), ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.

Die gSMC-K ist durch die gematik zugelassen.

Anwendungshinweis 30: In der Konnektor-Hardware werden physische gSMC-Ks verbaut.

A.NK.sichere_TI Sichere Telematikinfrastruktur-Plattform

Die zentrale Telematikinfrastruktur-Plattform und die damit verbundenen Netze werden als vertrauenswürdig angesehen, d.h., Angriffe aus der zentralen TI-Plattform sowie aus Netzen, die mit der zentralen TI-Plattform verbunden sind, werden nicht betrachtet.

Die Betreiber der Telematikinfrastruktur sorgen dafür, dass die Server in der Telematikinfrastruktur frei von Schadsoftware gehalten werden, so dass über den sicheren VPN-Kanal in den Konnektor hinein keine Angriffe erfolgen.

Die VPN-Schlüssel auf Seiten der VPN-Konzentratoren werden geheim gehalten und sind nur für die rechtmäßigen Administratoren zugänglich. Es werden weder VPN-Konzentratoren noch deren Schlüsselmaterial durch Angreifer entwendet.

Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

A.NK.kein_DoS Keine denial-of-service-Angriffe

Denial-of-service-Angriffe aus dem Transportnetz werden effektiv von Komponenten außerhalb des Konnektors abgewehrt.

Anwendungshinweis 31: Die Verantwortung für den Schutz der Systeme der zentralen Telematik-infrastruktur-Plattform bezüglich denial-of-service-Angriffe liegt bei den Firewall-Systemen im Perimeter der zentralen Telematikinfrastruktur-Plattform. Der Schwerpunkt der Abwehr durch den EVG beschränkt sich auf die in O.NK.PF_WAN und O.NK.PF_LAN beschriebenen Sicherheitsziele.

A.NK.AK Anwendungskonnektor nutzt EVG korrekt

Der Anwendungskonnektor nutzt die Sicherheitsdienste des EVG über dessen Schnittstellen automatisch. Durch die Art der Aufrufe ist für den EVG jederzeit eindeutig erkennbar, welche Daten über die VPN-Tunnel an die zentrale Telematikinfrastruktur-Plattform (offene und gesicherte Fachdienste, zentrale Dienste) und SIS weitergeleitet werden müssen.

Anwendungshinweis 32: Der Konnektor ist modular aufgebaut. Die einzelnen Module werden durch einen Security and Separation Layer (Virtualisierungsschicht) separiert. Neben der Hardware-Virtualisierung laufen die Module jeweils in eigenen Betriebssystems-Anwendungscontainern (Linux Container Umgebung). Die Kommunikation der Module untereinander wird durch ein dediziertes Firewall Modul geregelt. Daten die an die zentrale TI-Plattform und an den SIS weitergeleitet werden, sind daher strikt getrennt.

A.NK.CS Clientsystem nutzt EVG korrekt

Die Clientsysteme nutzen die Sicherheitsdienste des EVG über dessen Schnittstellen automatisch. Durch die Art der Aufrufe aus dem lokalen Netz des Leistungserbringers ist für den EVG jederzeit eindeutig erkennbar, welche Daten an Fachmodule und Basisdienste des Konnektors, über den VPN-Tunnel an die zentrale Telematikinfrastruktur-Plattform (offene Fachdienste, gesicherte Fachdienste, zentrale Dienste), die aktiven Bestandsnetze und den SIS weitergeleitet werden müssen.

Anwendungshinweis 33: Der Konnektor ist modular aufgebaut. Die einzelnen Module werden durch einen Security and Separation Layer (Virtualisierungsschicht) separiert. Neben der Hardware-Virtualisierung laufen die Module jeweils in eigenen Betriebssystems-Anwendungscontainern (Linux Container Umgebung). Die Kommunikation der Module untereinander wird durch ein dediziertes Firewall Modul geregelt. Daten die an die zentrale TI-Plattform, die aktiven Bestandsnetze und den SIS weitergeleitet werden, sind daher strikt getrennt.

A.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

Der Betreiber des Anwendungskonnektors organisiert dessen Betrieb in sicherer Art und Weise:

Er setzt nur gemäß dem Schutzprofil [12] zertifizierte Anwendungskonnektoren ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.

Er administriert die Anwendungskonnektoren in sicherer Art und Weise.

Er trägt die Verantwortung dafür, dass die Anwendungskonnektoren und Fachmodule den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

A.NK.Betrieb_CS Sicherer Betrieb der Clientsysteme

Der Betreiber der Clientsysteme organisiert diesen Betrieb in sicherer Art und Weise:

Er setzt nur Clientsysteme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.

Er administriert die Clientsysteme in sicherer Art und Weise.

Er trägt die Verantwortung dafür, dass die Clientsysteme den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

Er sorgt dafür, dass über Kanäle, die nicht der Kontrolle des Konnektors unterliegen (z. B. Einspielen von ausführbaren Dateien über lokale optische Laufwerke oder über USB-Stick, Öffnen von E-Mail-Anhängen) keine Schadsoftware auf die Clientsysteme oder andere IT-Systeme im LAN aufgebracht wird.

Er ist verantwortlich dafür, dass eine Anbindung der Clientsysteme an potentiell unsichere Netze (z. B. Internet) unterbunden wird oder ausschließlich in sicherer Art und Weise erfolgt. Die Anbindung an unsichere Netze kann z. B. dadurch in sicherer Art und Weise erfolgen, dass es neben dem definierten Zugang zum Transportnetz über den EVG keine weiteren ungeschützten oder schlechter geschützten Zugänge zum Transportnetz gibt.

Die Verantwortung für die Clientsysteme liegt sowohl beim Leistungserbringer (der z. B. lokal potentiell bösartige Software oder auch potentiell fehlerhafte Updates der Clientsystem-Software einspielen könnte) als auch beim Clientsystem-Hersteller (der z. B. den korrekten Aufruf der Konnektor-Schnittstellen sicherstellen muss).

A.NK.Admin_EVG Sichere Administration des EVG

Der Betreiber des EVG sorgt dafür, dass administrative Tätigkeiten (dies umfasst sowohl die lokale als auch die optionale zentrale Administration) in Übereinstimmung mit der Administrator-Dokumentation des EVG durchgeführt werden. Insbesondere ist für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal einzusetzen. Die Administratoren halten Authentisierungsinformationen und –token geheim bzw. geben diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token).

A.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

Es sind sichere Ersatzverfahren etabliert, auf die zurückgegriffen werden kann, wenn wenn plötzliche Schwächen in den verwendeten kryptographischen Algorithmen bekannt werden, die nicht durch die redundanten Algorithmen ausgeglichen werden können.

A.NK.Zugriff_gSMC-K Effektiver Zugriffsschutz auf gSMC-K

Es sind effektive Zugriffsschutzmaßnahmen etabliert, die den möglichen Zugriff von Komponenten des Konnektors auf Schlüsselmaterial der gSMC-K kontrollieren und unzulässige Zugriffe verhindern. Die Zugriffskontrolle kann durch eine zentrale Instanz vermittelt werden oder es wird sichergestellt, dass die Komponenten des Konnektors nur auf ihr eigenes Schlüsselmaterial zugreifen.

Anwendungshinweis 34: Dieser Aspekt wird im PP [12] des Gesamtkonnektors als übergreifende Sicherheitsfunktion modelliert.

4. Sicherheitsziele

Die hier definierten Sicherheitsziele wurden entsprechend zum zugrundeliegenden PP mit dem zusätzlichen Kürzel „NK“ versehen. Damit wird die Herkunft dieser Artefakte eindeutig mit „Netzkonnektor“ gekennzeichnet.

4.1. Sicherheitsziele für den EVG

Der EVG schützt die Nutzdaten (Benutzerdaten / *User Data* im Sinne der Common Criteria: zu schützende Daten der TI und der Bestandsnetze (siehe Abschnitt 3.1), die Clientsysteme und die TSF Daten.

4.1.1. Allgemeine Ziele: Schutz und Administration

O.NK.TLS_Krypto TLS-Kanäle mit sicheren kryptographischen Algorithmen

Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [18]. Zudem prüft der EVG die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

Anwendungshinweis 35: Für welche Verbindungen TLS-Kanäle genutzt werden, ist Gegenstand des Anwendungskonnektors. Der Netzkonnektor stellt die kryptographische Grundfunktionalität für TLS zur Verfügung.

O.NK.Schutz Selbstschutz, Selbsttest und Schutz von Benutzerdaten

Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten. Der EVG schützt sich selbst gegen sicherheitstechnische Veränderungen an den äußeren logischen Schnittstellen bzw. erkennt diese oder macht diese erkennbar.

Der EVG erkennt bereits Versuche, sicherheitstechnische Veränderungen durchzuführen, sofern diese über die äußeren Schnittstellen des EVGs erfolgen (mit den unter OE.NK.phys_Schutz formulierten Einschränkungen).

Der EVG führt beim Start-up und bei Bedarf Selbsttests durch.

Der EVG löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden.

Anwendungshinweis 36: Annahmen zum physischen Schutz: Der Schutz vor physischen Angriffen wird durch die Einsatzumgebung gewährleistet (siehe A.NK.phys_Schutz). Der EVG selbst besteht nur aus der Software des Netzkonnektors.

O.NK.EVG_Authenticity Authentizität des EVG

Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können. Gefälschte EVGs müssen vom VPN-Konzentrator sicher erkannt werden können. Der EVG muss auf Anforderung und mit Unterstützung der gSMC-K einen Nachweis seiner Authentizität ermöglichen.

Anwendungshinweis 37: Die Auslieferung des Netzkonnektor gegenüber dem empfangenden Leistungserbringer oder dem von ihm beauftragten Servicetechniker erfolgt durch gesicherten Transport. Nach Erhalt des Netzkonnektors muss dieser bis zur Inbetriebnahme in einem gesicherten Bereich aufbewahrt werden. Der Betrieb selbst findet in einer sicheren Umgebung statt (siehe OE.NK.phys_Schutz). Die Authentizität des EVG wird dadurch nachgewiesen, dass der Netzkonnektor sich erfolgreich gegenüber einem VPN-Konzentrator für Dienste gemäß § 291 a SGB V [9] authentisiert hat und fachliche Anwendungsfälle im Online-Modus durchgeführt werden können.

O.NK.Admin_EVG Administration nur nach Autorisierung und über sicheren Kanal

Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen.

Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung eines Administrators, welcher die lokale und-entfernte Administration des EVG durchführen kann. Die Administration erfolgt rollenbasiert.

Weil die Administration über Netzverbindungen (lokal über PS2 oder zentral über PS3) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).

Der EVG verhindert die Administration folgender Firewall-Regeln:

- Regeln für die Kommunikation zwischen Konnektor und Transportnetz,
- Regeln für die Kommunikation zwischen Konnektor und Telematikinfrastruktur, sowohl gesicherte als auch offene Fachdienste und zentrale Dienste,
- Regeln für die Kommunikation zwischen Konnektor und den Bestandsnetzen,
- Regeln für die Kommunikation zwischen LAN und dem Transportnetz,
- Regeln für die Kommunikation zwischen LAN und der Telematikinfrastruktur, sowohl gesicherte als auch offene Fachdienste und zentrale Dienste,
- Regeln für die Kommunikation zwischen LAN und den Bestandsnetzen (außer Freischalten aktiver Bestandsnetze),

Anwendungshinweis 38: Der EVG unterstützt die Rolle Administrator. Dabei wird TOE-intern zwischen den Administrator-Rollen *local administrator* und *super administrator* unterschieden. Der lokale Administrator kann den TOE über die jeweilige Schnittstelle konfigurieren. Der Super Adminsistrator hat kann zudem die Benutzerkonten verwalten. Dazu gehört die Vergabe von Zugriffsrechten bezüglich der Konfigurationsbereiche und zum Werksreset. Die Super-Administrierung erfolgt über die lokale Schnittstelle (LAN). Es können alle Management-Funktionen der TSF von den Administratoren ausgeführt werden. Daher werden unter dem Subjekt Adminsitrator die einzelnen Rollen zusammengefasst. Der EVG nimmt die Authentifizierung selbst vor; O.NK.Admin_EVG wurde aus dem PP [11] übernommen und geeignet verschärft. Die Anpassungen zum PP wurden durch durchgestrichenen Text kenntlich gemacht.

Anwendungshinweis 39: Jede Änderung, die ein Administrator vornimmt, wird zusammen mit einem Zeitstempel und der Identität des Administrators protokolliert.

Anwendungshinweis 40: Der für die Administration notwendige sichere logische Kanal beruht auf den durch [18] vorgegebenen Protokollen und Algorithmen.

O.NK.Admin_Auth Der Netzkonnektor führt die Authentisierung des Administrators durch.

Anmerkung: Das Umgebungsziel OE.NK.Admin_Auth aus dem Protection Profile [11] wurde in ein Sicherheitsziel des EVG umgewandelt.

O.NK.Protokoll **Protokollierung mit Zeitstempel**

Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit.

Anwendungshinweis 41: Der für das Protokoll erforderliche Zeitstempel wird dabei durch O.NK.Zeitdienst bereitgestellt.

Anwendungshinweis 42: Eine Protokollierung von Zugriffen auf medizinische Daten nach § 291 a (6) Satz 2 SGB V erfolgt durch den Anwendungskonnektor (auf der eGK oder in der zentralen Telematikinfrastruktur-Plattform). Diese Art der Protokollierung ist hier nicht gemeint; der EVG ist in die Protokollierung von Zugriffen auf medizinische Daten nicht involviert.

O.NK.Zeitdienst **Zeitdienst**

Der EVG synchronisiert die Echtzeituhr gemäß OE.NK.Echtzeituhr in regelmäßigen Abständen über einen sicheren Kanal mit einem vertrauenswürdigen Zeitdienst (siehe OE.NK.Zeitsynchro).

Anwendungshinweis 43: Die sichere Systemzeit wird u. a. für die Gültigkeitsprüfung von Zertifikaten von VPN-Konzentratoren verwendet.

O.NK.Update **Software Update**

Bevor Updatedaten für den EVG oder andere Komponenten bereitgestellt werden, muss die Integrität und die Authentizität / Zulässigkeit der Updatedaten überprüft (Signaturprüfung und Prüfung der Identität des Signierenden) und Metadaten (zum Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen) angezeigt

werden. Schlägt die Prüfung der Integrität fehl, verhindert der EVG die Bereitstellung der Updatedaten. Die Installation dieser Updates kann durch den Administrator oder, wenn dies vom Administrator explizit so konfiguriert wurde, automatisch erfolgen.

Hinweis: O.NK.Update wurde von O.AK.Update aus dem Protection Profile BSI-CC-PP-0098-V3-2021-MA-03 [12] abgeleitet und bezieht sich auf das Update der Software des Konnektors, nicht jedoch auf die Updates von TSL, CRL und BNetzA-VL. Die Updatefunktion für Software wird komplett durch den EVG implementiert und daher wurden alle SFRs, die laut BSI-CC-PP-0098-V3-2021-MA-03 [12], Abschnitt 6.5.5 dem Aspekt Update der Software zugeordnet sind, in diese Sicherheitsvorgaben übernommen. Im Einzelnen sind diese SFRs in der folgenden Tabelle gelistet:

Bezeichner in BSI-CC-PP-0098-V3-2021-MA-03 [12]	**Bezeichner in diesen Sicherheitsvorgaben**
FDP_ACC.1/AK.Update	FDP_ACC.1/NK.Update
FDP_ACF.1/AK.Update	FDP_ACF.1/NK.Update
FDP_UIT.1/AK.Update	FDP_UIT.1/NK.Update
FTP_ITC.1/AK.KSR	FTP_ITC.1/NK.KSR

Zum Erfüllen aller Abhängigkeiten dieser hinzugefügten SFRs waren keine weiteren SFRs notwendig, da exakt wie in der Begründung der Nichterfüllung zu FMT_MSA.3 in BSI-CC-PP-0098-V3-2021-MA-03 [12] der EVG keine Initialisierung von Sicherheitsattributen im Zusammenhang zu Software-Updates durchführt.

Die Updatefunktion für Software kann auch für das Nachladen von geprüften und freigegebenen Fachmodulen verwendet werden.

4.1.2. Ziele für die VPN-Funktionalität

O.NK.VPN_Auth Gegenseitige Authentisierung für den VPN-Tunnel

Der EVG erzwingt die Authentisierung der Kommunikationspartner der VPN-Tunnel (VPN-Konzentratoren der TI und des SIS) und ermöglicht eine Authentisierung seiner selbst gegenüber den VPN-Konzentratoren in der zentralen Telematikinfrastruktur-Plattform und des SIS.

Der EVG prüft zertifikatsbasiert die Authentizität der VPN-Konzentratoren der TI und des SIS.

Der EVG authentisiert sich gegenüber den VPN-Konzentratoren der TI und des SIS. Das dazu erforderliche Schlüsselmaterial bezieht der EVG von der gSMC-K.

Außerdem überprüft der EVG, dass die verwendeten Algorithmen gemäß *Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung*, Teil 1: Telematikinfrastruktur [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [18] noch gültig sind.

Anwendungshinweis 44: Der EVG implementiert die Algorithmen nach TR-03116-1 [14]. Eine Prüfung der Gültigkeit der Algorithmen wird nicht explizit durchgeführt. Die Gültigkeit wird im Rahmen der Evaluierung des Netzkonnektors sichergestellt. Weiterhin bietet der EVG keine Funktionalität die Verfügbarkeit der in Bezug auf die benannten Spezifikationen ungültigen Algorithmen selektiv einzuschränken. Eine Einschränkung der im Konnektor verwendbaren Algorithmen wird über ein Software-Update durchgesetzt.

O.NK.Zert_Prüf Gültigkeitsprüfung für VPN-Zertifikate

Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form einer CRL und einer TSL bereitgestellt.

O.NK.VPN_Vertraul Schutz der Vertraulichkeit von Daten im VPN-Tunnel

Der EVG schützt die Vertraulichkeit der Nutzdaten[20] bei der Übertragung von und zu den VPN-Konzentratoren.

Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren verschlüsselt (vor dem Versand) bzw. entschlüsselt (nach dem Empfang) der Konnektor die Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.

Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.

O.NK.VPN_Integrität Integritätsschutz von Daten im VPN-Tunnel

Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren.

Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.

[20] Der Begriff „Nutzdaten“ schließt in diesem PP grundsätzlich auch die Verkehrsdaten mit ein, also auch Daten über Kommunikationsbeziehungen – beispielsweise Daten darüber, welcher Versicherte zu welchem Zeitpunkt bei welchem HBA-Inhaber Leistungen in Anspruch genommen hat.

4.1.3. Ziele für die Paketfilter-Funktionalität

O.NK.PF_WAN Dynamischer Paketfilter zum WAN

Der EVG schützt sich selbst und andere Konnektorteile vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN). Wenn der Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt[21], dann schützt der EVG auch die Clientsysteme.

Der EVG ermöglicht die Kommunikation von aktiven Komponenten im LAN des LE mit dem SIS.

Mit Ausnahme der Kommunikation der Clientsysteme mit den Bestandsnetzen und den offenen Fachdiensten wird grundsätzlich jeder nicht vom Konnektor generierte, direkte Verkehr aus dem LAN in den VPN-Tunnel zur TI ausgeschlossen. Es werden Angreifer mit hohem Angriffspotential betrachtet.

Anwendungshinweis 45: Die Inhalte der Kommunikation über den VPN-Tunnel werden vom Konnektor nicht ausgewertet.

O.NK.PF_LAN Dynamischer Paketfilter zum LAN

Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN). Es werden Angreifer mit hohem Angriffspotential betrachtet.

Für zu schützende Daten der TI und der Bestandsnetze sowie *zu schützende Nutzerdaten* bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Clientsystemen) auf das Transportnetz wird durch den EVG unterbunden: IT-Systeme im LAN können nur unter der Kontrolle des EVG und im Einklang mit der Sicherheitspolitik des EVG zugreifen.

Anwendungshinweis 46: Siehe auch OE.NK.AK.

O.NK.Stateful Stateful Packet Inspection (zustandsgesteuerte Filterung)

Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter.

[21] Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [16], Kapitel 2.7.

4.2. Sicherheitsziele für die Umgebung

Die Einsatzumgebung des EVG (IT-Umgebung oder non-IT-Umgebung) muss folgende Sicherheitsziele erfüllen:

OE.NK.RNG Externer Zufallszahlengenerator

Die Umgebung stellt dem EVG einen externen Zufallszahlengenerator bereit, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klassen PTG.2 oder PTG.3 aus [8] liefert.

Anwendungshinweis 47: Der Zufallszahlengenerator der gSMC-K wird als physikalischer Zufallszahlengenerator der Klasse PTG.2 als (Re-)Seed-Generator für den Zufallszahlengenerator des Betriebssystems genutzt.

OE.NK.Echtzeituhr Echtzeituhr

Die IT-Umgebung stellt dem EVG eine Echtzeituhr zur Verfügung, die gemäß O.NK.Zeitdienst synchronisiert werden kann. Die Echtzeituhr erfüllt die relevanten Anforderungen zur Freilaufgenauigkeit.

Anwendungshinweis 48: Die Hardware-Platform des Netzkonnektors muss eine Real Time Clock mit maximale zulässigem Fehler von +/- 20ppm (part per million) zur Verfügung stellen. Dies entspricht einer maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über 20 Tage. Die Freilaufgenauigkeit garantiert eine Abweichung von weniger als 2 Sekunden pro Tag, so dass bei einer Synchronisation spätestens alle 24 Stunden der Zeitdienst des Konnektors um maximal 2 Sekunden ungenau ist.

OE.NK.Zeitsynchro Zeitsynchronisation

Die IT-Umgebung (zentrale Telematikinfrastruktur-Plattform) stellt einen Dienst bereit (Zeitserver, die über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur erreichbar sind), mit deren Hilfe der EVG die Echtzeituhr gemäß OE.NK.Echtzeituhr synchronisieren kann. Dieser Dienst muss über eine verlässliche Systemzeit verfügen, über einen sicheren Kanal erreichbar sein (Zeitserver stehen innerhalb der Telematikinfrastruktur) und hinreichend hoch verfügbar sein.

OE.NK.gSMC-K Sicherheitsmodul gSMC-K

gSMC-K sicher verbunden

Der EVG hat Zugriff auf ein Sicherheitsmodul gSMC-K, das sicher mit dem EVG verbunden ist. Sicher bedeutet in diesem Fall, dass die gSMC-K nicht unbemerkt vom EVG getrennt werden kann und dass die Kommunikation zwischen gSMC-K und EVG weder mitgelesen noch manipuliert werden kann.

Die gSMC-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des EVG repräsentiert und welches auch für O.NK.VPN_Auth verwendet wird, und führt kryptographische Operationen mit diesem Schlüsselmaterial durch

(Authentisierung), ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.

Die gSMC-K stellt Zufallszahlen zur Schlüsselerzeugung bereit, die von einen Zufallszahlengenerator der Klasse PTG.2 oder PTG.3 erzeugt wurden.

Außerdem enthält die gSMC-K Schlüsselmaterial zur Verifikation der Authentizität des VPN-Konzentrators.

Anwendungshinweis 49: Das Betriebssystem der integrierten gSMC-K ist von der gematik zugelassen.

OE.NK.KeyStorage Sicherer Schlüsselspeicher

Die IT-Umgebung (ein Teil des Gesamtkonnektors) stellt dem EVG einen sicheren Schlüsselspeicher bereit. Der sichere Schlüsselspeicher schützt sowohl die Vertraulichkeit als auch die Integrität des in ihm gespeicherten Schlüsselmaterials.

Der Schlüsselspeicher wird vom NK verwendet zur Speicherung von privaten Schlüsseln, die zur Authentisierung beim Aufbau des VPN-Tunnels verwendet werden (kryptographische Identität des EVG, siehe FTP_ITC.1/NK.VPN_TI) oder im Rahmen des TLS-Verbindungsaufbaus (siehe FTP_ITC.1/NK.TLS). Zudem unterstützt der Schlüsselspeicher den EVG bei der sicheren Speicherung von Geheimnissen, wie zum Beispiel Sitzungsschlüssel (session keys).

Anwendungshinweis 50: Der Netzkonnektor stellt ein symmetrisch verschlüsseltes Filesystem (Crypted File System, CFS) als Datenspeicher für sichere Speicherung von Geheimnissen zur Verfügung. Der symmetrische Schlüssel selbst wird durch einen asymmetrischen Schlüssel der in der gSMC-K („sicherer Schlüsselspeicher“) hinterlegt ist geschützt.

Anwendungshinweis 51: Der Schlüsselspeicher wird auch zur Speicherung von

- Prüfschlüsseln (öffentlicher Schlüssel) zur Verifikation der eigenen Integrität,
- Prüfschlüsseln (öffentlicher Schlüssel) zur Verifikation der Authentizität von Software-Updates,
- Geheimnissen (Passwörtern), mit denen der Administrator sich gegenüber dem EVG authentisieren kann (FTP_TRP.1/NK.Admin), sowie vom
- DNSSEC Vertrauensanker der TI (DNSSEC wird vom DNS-Dienst des EVG unterstützt)

verwendet.

OE.NK.AK Korrekte Nutzung des EVG durch Anwendungskonnektor

Anwendungskonnektoren müssen zu schützende Daten der TI und der Bestandsnetze, die durch Dienste gemäß § 291a SGB V [9] verarbeitet werden sollen, in korrekter Weise an den EVG übergeben, damit der EVG zu schützende Daten der TI und der Bestandsnetze über den entsprechenden VPN-Tunnel für Dienste gemäß § 291a SGB V versenden kann.

Dazu müssen die Anwendungskonnektoren die vom EVG bereitgestellten Schnittstellen geeignet verwenden, so dass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

Anwendungshinweis 52: Siehe auch A.NK.AK.

OE.NK.CS Korrekte Nutzung des Konnektors durch Clientsysteme und andere aktive Komponenten im LAN

Die Hersteller von Clientsystemen müssen ihre Produkte so gestalten, dass diese den Konnektor für Dienste gemäß § 291a SGB V [9] korrekt aufrufen. Aufrufe von Diensten gemäß § 291a SGB V [9] müssen über den Anwendungskonnektor erfolgen. Der Zugriff auf Bestandsnetze und offene Fachanwendungen erfolgt nur durch aktive Komponenten im LAN in den vorgesehenen IP-Adressbereichen.

OE.NK.Admin_EVG Sichere Administration des Netzkonnektors

Der Betreiber des Netzkonnektors muss dafür sorgen, dass administrative Tätigkeiten der lokalen und zentralen Administration in Übereinstimmung mit der Administrator-Dokumentation des EVGs durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen und –token (z. B. PIN bzw. Passwort oder Schlüssel-Token) geheim halten bzw. dürfen diese nicht weitergeben. Wenn ein Konnektor und/oder sein Sicherheitsmodul gSMC-K gestohlen wird oder abhandenkommt, muss der Betreiber des EVGs den Betreiber der PKI (vgl. OE.NK.PKI) informieren. Dazu muss sichergestellt sein, dass gestohlene oder abhanden gekommene Geräte (gSMC-K oder NK) eindeutig identifiziert werden können.

Anwendungshinweis 53: Der EVG hat eine Seriennummer über die eine Identifikation erfolgen kann. Es wird organisatorisch sichergestellt, dass die Seriennummer bei Verlust des Gerätes noch vorliegt oder rekonstruiert werden kann, damit das Gerät bei der Verlustmeldung eindeutig identifiziert werden kann und weitergehende Schritte (z. B. Sperrung des zugehörigen Zertifikats) eingeleitet werden können.

Anwendungshinweis 54: Der EVG führt die Authentisierung selbst durch. Das Umgebungsziel OE.NK.Admin_Auth aus dem PP [11] wurde in ein EVG-Ziel O.NK.Admin_Auth umgewandelt und wird in diesem ST daher nicht mehr aufgeführt. OE.NK.Admin_Auth kann als automatisch durch O.NK.Admin_Auth erfüllt angesehen werden. Die funktionale Anforderung FMT_MSA.4/NK wird beibehalten, da die Anforderung, dass nur bei erfolgreicher Autorisierung ein entsprechender Sicherheitszustand gesetzt wird, nach wie vor gültig ist.

OE.NK.PKI Betrieb einer Public-Key-Infrastruktur und Verteilung der TSL

Die Umgebung muss eine Public-Key-Infrastruktur bereitstellen, mit deren Hilfe der EVG im Rahmen der gegenseitigen Authentisierung die Gültigkeit der zur Authentisierung verwendeten Zertifikate prüfen kann. Dazu stellt die Umgebung Zertifikate zulässiger VPN-Konzentratoren für den Zugang in die Telematikinfrastruktur bereit bzw. Zertifikate der ausstellenden CAs.

Wird eine Kompromittierung, Betriebsaufgabe oder Vertragsbeendigung eines VPN-Konzentrators, des Schlüsselmaterials eines VPN-Konzentrators, einer CA oder des Schlüsselmaterials einer CA bekannt, so reagiert der Betreiber der PKI geeignet, indem er je nach Erfordernis das zugehörige Zertifikat (des VPN-Konzentrators oder der CA) sperrt und diese Information (z. B. in Form einer Sperrliste (CRL)) für die Konnektoren bereitstellt, so dass EVGs mit kompromittierten VPN-Konzentratoren keine Verbindung mehr aufbauen.

Meldet ein Konnektor-Betreiber seinen Konnektor und/oder dessen Sicherheitsmodul gSMC-K als gestohlen oder anderweitig abhandengekommen, so sperrt der Betreiber der PKI das zugehörige Zertifikat und stellt diese Information (über eine CRL) für die VPN-Konzentratoren bereit, so dass diese mit dem abhanden gekommenen Konnektor keine Verbindung mehr aufbauen.

OE.NK.phys_Schutz Physischer Schutz des EVG

Die Sicherheitsmaßnahmen in der Umgebung müssen den Konnektor (während aktiver Datenverarbeitung im Konnektor) vor physischen Zugriff Unbefugter schützen. Befugt sind dabei nur durch den Betreiber des Konnektors namentlich autorisierte Personen (z. B. Leistungserbringer, ggf. medizinisches Personal). Sowohl während als auch außerhalb aktiver Datenverarbeitung im Konnektor müssen die Sicherheitsmaßnahmen in der Umgebung sicherstellen, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass die einzuleitenden materiellen, organisatorischen und/oder personellen Maßnahmen größeren Schaden abwehren.

Im Fall eines verteilt betriebenen Mehrkomponenten-Konnektors muss die Umgebung außerdem den Kommunikationskanal zwischen den

Konnektorteilen Anwendungskonnektor und Netzkonnektor, sowie dem EVG und weiteren Komponenten des Konnektors während aktiver Datenverarbeitung vor physischem Zugriff schützen und außerhalb aktiver Datenverarbeitung physische Manipulation erkennen.

Anwendungshinweis 55: Siehe auch A.NK.phys_Schutz.

OE.NK.sichere_TI Sichere Telematikinfrastruktur-Plattform

Die Betreiber der zentralen Telematikinfrastruktur-Plattform müssen sicherstellen, dass aus dem Netz der zentralen TI-Plattform heraus keine Angriffe gegen den Konnektor durchgeführt werden. Das schließt auch Angriffe auf den Konnektor oder auf die lokalen Netze der Leistungserbringer aus weiteren Netzen ein, die mit der TI verbunden sind (Bestandsnetze).

Die Betreiber der Telematikinfrastruktur müssen dafür sorgen, dass die Server in der Telematikinfrastruktur frei von Schadsoftware gehalten werden, so dass über den sicheren VPN-Kanal in den Konnektor hinein keine Angriffe erfolgen. Dies impliziert, dass die VPN-Schlüssel auf Seiten des VPN-Konzentrators geheim gehalten werden müssen und nur für die rechtmäßigen Administratoren zugänglich sein dürfen.

Alle Administratoren in der Telematikinfrastruktur müssen fachkundig und vertrauenswürdig sein.

OE.NK.kein_DoS Keine denial-of-service-Angriffe

Die Betreiber der zentralen Telematikinfrastruktur-Plattform müssen geeignete Gegenmaßnahmen treffen, um denial-of-service Angriffe aus dem Transportnetz gegen die Telematikinfrastruktur abzuwehren.

Anwendungshinweis 56: Siehe auch A.NK.kein_DoS.

OE.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

Der Betreiber des Anwendungskonnektors muss diesen Betrieb in sicherer Art und Weise organisieren:

Er administriert die Anwendungskonnektoren in sicherer Art und Weise.

Er trägt die Verantwortung dafür, dass die Anwendungskonnektoren und Fachmodule den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

OE.NK.Betrieb_CS Sicherer Betrieb der Clientsysteme

Der Betreiber der Clientsysteme muss diesen Betrieb in sicherer Art und Weise organisieren:

Er setzt nur Clientsysteme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.

Er administriert die Clientsysteme in sicherer Art und Weise.

Er trägt die Verantwortung dafür, dass die Clientsysteme den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

Er sorgt dafür, dass über Kanäle, die nicht der Kontrolle des Konnektors unterliegen (z. B. Einspielen von ausführbaren Dateien über lokale optische Laufwerke oder über USB-Stick, Öffnen von E-Mail-Anhängen) keine Schadsoftware auf die Clientsysteme oder andere IT-Systeme im LAN aufgebracht wird.

Er ist verantwortlich dafür, dass eine Anbindung der Clientsysteme an potentiell unsichere Netze (z. B. Internet) unterbunden wird oder ausschließlich in sicherer Art und Weise erfolgt. Die Anbindung an unsichere Netze kann z. B. dadurch in sicherer Art und Weise erfolgen, dass es neben dem definierten Zugang zum Transportnetz über den EVG keine weiteren ungeschützten oder schlechter geschützten Zugänge zum Transportnetz gibt.

Die Verantwortung für die Clientsysteme liegt sowohl beim Leistungserbringer (der z. B. lokal potentiell bösartige Software oder auch potentiell fehlerhafte Updates der Clientsystem-Software einspielen könnte) als auch beim Clientsystem-Hersteller (der z. B. den korrekten Aufruf der Konnektor-Schnittstellen sicherstellen muss).

OE.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

Es müssen sichere Ersatzverfahren etabliert werden, auf die zurückgegriffen werden kann, wenn plötzliche Schwächen in den verwendeten kryptographischen Algorithmen bekannt werden, die nicht durch die redundanten Algorithmen ausgeglichen werden können.

OE.NK.SIS Sicherer Internet Service

Die Umgebung stellt einen gesicherten Zugangspunkt zum Internet bereit. Dieser Zugangspunkt muss die dahinter liegenden Netze der Benutzer wirksam gegen Angriffe aus dem Internet schützen.[22]

Die Administration des Sicheren Internet Service muss dafür sorgen, dass dieses System frei von Schadsoftware gehalten wird, so dass keine Angriffe über den sicheren VPN-Kanal zum Konnektor von diesem Zugangspunkt ausgehen. Im Fall der Nutzung des SIS als VPN-

[22] Es wird darauf hingewiesen, dass ein absoluter Schutz der Netze vor Angriffen aus dem Internet durch einen gesicherten Zugangspunkt praktisch nicht realisierbar ist. Als Folge muss der Schutz der Clientsysteme stets auch weitere Maßnahmen umfassen. In diesem Security Target wird daher eine Kombination aus einem gesicherten Zugangspunkt zum Internet (OE.NK.SIS) und lokalen Schutzmaßnahmen auf den Clientsystemen (OE.NK.Betrieb_CS) gefordert.

Konzentrator[23] impliziert dies, dass die VPN-Schlüssel auf Seiten des Sicheren Internet Service geheim gehalten werden müssen und nur für die rechtmäßigen Administratoren zugänglich sein dürfen.

Alle Administratoren des Sicheren Internet Service müssen fachkundig und vertrauenswürdig sein.

OE.NK.SW-Update Prozesse für sicheres Software-Update

Die Einsatzumgebung etabliert Prozesse, die dafür sorgen, dass Update-Pakete und nachzuladende Fachmodule für den EVG nur dann signiert und ausgeliefert werden, wenn der Code von einer dazu autorisierten Stelle geprüft und freigegeben wurde. Zertifizierte EVG-Komponenten dürfen nur durch zertifizierte Komponenten ersetzt werden.

Hinweis: OE.NK.SW-Update wurde von OE.SW-Update aus dem Protection Profile BSI-CC-PP-0098-V3-2021-MA-03 [12] abgeleitet.

[23] Laut Konnektor-Spezifikation (Kapitel 2.7) [16] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

4.3. Erklärung der Sicherheitsziele (Security Objectives Rationale)

4.3.1. Überblick: Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele

Die folgende Tabelle 7 bildet die Bedrohungen (Threats), organisatorischen Sicherheitspolitiken (OSPs) und Annahmen (Assumptions) auf Sicherheitsziele für den EVG und die Umgebung ab.

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.NK.TLS_**Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	O.NK.Admin_Auth	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.gSMC-K	OE.NK.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.PKI	OE.NK.phys_Schutz	OE.NK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betrieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS	OE.NK.SW-Update
T.NK.local_EVG_LAN		X			X	X							X				X	X		X												
T.NK.remote_EVG_WAN		X			X	X		X	X		X	X		X		X	X	X	X	X				X		X				X		
T.NK.remote_EVG_LAN		X			X	X		X	X		X	X	X	X		X		X	X	X				X		X			X	X	X	
T.NK.remote_VPN_Data						X		X	X	X	X					X		X	X	X	X			X		X		X	X	X	X	
T.NK.local_admin_LAN		X		X	X	X									X	X		X		X			X								
T.NK.remote_admin_WAN		X		X	X	X									X	X		X		X			X								
T.NK.counterfeit			X																X						X					X		
T.NK.Zert_Prüf									X															X						X		
T.NK.TimeSync						X		X	X		X					X		X	X					X						X		
T.NK.DNS								X	X															X					X	X		
OSP.NK.Zeitdienst						X											X	X														
OSP.NK.SIS												X																			X	
OSP.NK.BOF								X	X	X	X	X		X									X									
OSP.NK.TLS	X																															
OSP.NK.SW-Update				X	X		X																									X
A.NK.phys_Schutz																									X							
A.NK.gSMC-K																			X													
A.NK.sichere_TI																										X						

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.NK.TLS_**Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	O.NK.Admin_Auth	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsvnchro	OE.NK.gSMC-K	OE.NK.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.PKI	OE.NK.phys_Schutz	OE.NK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betrieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS	OE.NK.SW-Update
A.NK.kein_DoS																											X					
A.NK.AK																					X											
A.NK.CS																						X										
A.NK.Betrieb_AK																												X				
A.NK.Betrieb_CS																													X			
A.NK.Admin_EVG																							X									
A.NK.Ersatzverfahren																														X		
A.NK.Zugriff_gSMC-K																			X									X				

Tabelle 7: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen

Ein Kreuz „X“ in einer Zelle bedeutet, dass die in der Zeile des Kreuzes stehende Bedrohung durch das in der Spalte des Kreuzes stehende Sicherheitsziel (für den EVG oder für die Umgebung) abgewehrt wird bzw. dass die in der Zeile des Kreuzes stehende Annahme auf das entsprechende Umgebungsziel abgebildet wird. Man beachte, dass Common Criteria die Abbildung von Annahmen auf EVG-Sicherheitsziele verbietet; der entsprechende Bereich der Tabelle ist daher grau schattiert.

Die Abwehr einiger Bedrohungen wird zusätzlich zu den benannten Sicherheitszielen durch Assurance-Komponenten unterstützt:

Die Abwehr von T.NK.local_EVG_LAN wird durch die Klasse ADV und die Familie AVA_VAN unterstützt.

Die Abwehr von T.NK.counterfeit wird durch die Komponenten ALC_DEL.1 und AGD_OPE.1 unterstützt.

Das Ziel OE.NK.Admin_EVG wird durch die Familie AGD_OPE unterstützt.

Anwendungshinweis 57: Sämtliche Bedrohungen, organisatorische Sicherheitspolitiken und Annahmen, sowie die Sicherheitsziele wurden aus dem Protection Profile [11] übernommen. Entsprechend ist auch die Erklärung zu den Sicherheitszielen aus dem PP übernommen. Im PP werden dabei optionale Abbildungen von Sicherheitszielen auf Bedrohungen angegeben. Diese werden in Tabelle 4 des PPs als in Klammern gesetztes kleines Kreuz (x) dargestellt. In diesem ST wurden keine optionalen Beziehungen ausgewählt und die in Klammern gesetzten kleinen Kreuze (x) wurden aus der Tabelle entfernt. Es wurden keine Beziehungen ergänzt.

4.3.2. Abwehr der Bedrohungen durch die Sicherheitsziele

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 7 auf die Bedrohungen abgebildeten Sicherheitsziele geeignet sind, um die Bedrohungen abzuwehren.

4.3.2.1. T.NK.local_EVG_LAN

T.NK.local_EVG_LAN greift den EVG über seine LAN-Schnittstelle an. Der EVG filtert alle Nachrichten, die ihn auf dieser Schnittstelle erreichen, mit Hilfe des LAN-seitigen Paketfilters (O.NK.PF_LAN; mit grundlegender zustandsgesteuerter Filterungs-Funktionalität); dieser schützt den EVG vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer. Der EVG schützt auch den Anwendungskonnektor vor LAN-seitigen Angriffen (O.NK.PF_LAN) und trägt somit zur Abwehr der Bedrohung bei. Der dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) protokolliert werden (z. B. die letzte vorgenommene Konfigurationsänderung), und von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

4.3.2.2. T.NK.remote_EVG_WAN

T.NK.remote_EVG_WAN beschreibt einen Angriff aus dem Transportnetz, bei dem der EVG bzw. dessen Integrität bedroht wird. Angriffe aus dem Transportnetz werden durch den VPN-Tunnel und den Paketfilter mit Stateful Packet Inspection (zustandsgesteuerte Filterung) abgewehrt: Anfragen, die ein Angreifer mit Hilfe des VPN-Tunnels zu senden versucht, werden vom EVG als ungültig erkannt (weil der Angreifer die VPN-Schlüssel nicht kennt, O.NK.VPN_Integrität) und verworfen. Die gSMC-K speichert das für die Authentisierung des VPN-Kanals erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die Inhalte, die durch den VPN-Tunnel übertragen werden, sind nicht bösartig (OE.NK.sichere_TI). Anfragen außerhalb des VPN-Tunnels werden durch den dynamischen Paketfilter gefiltert (O.NK.PF_WAN) – der EVG schützt sich selbst mittels des WAN-seitigen Paketfilters. Der WAN-seitige Paketfilter bietet zustandsgesteuerte Filterung (stateful packet inspection, zustandsgesteuerte Filterung, O.NK.Stateful). Der dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) protokolliert werden (z. B. die letzte vorgenommene Konfigurationsänderung), und von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

Außerdem authentisieren sich die VPN-Partner gegenseitig zu Beginn der Kommunikation (O.NK.VPN_Auth). Im Rahmen der gegenseitigen Authentisierung wird eine Zertifikatsprüfung durchgeführt (O.NK.Zert_Prüf), die wiederum eine entsprechende PKI in der Umgebung voraussetzt (OE.NK.PKI). Im Rahmen der Gültigkeitsprüfung von Zertifikaten benötigt der EVG eine sichere Zeitquelle (O.NK.Zeitdienst und regelmäßige Synchronisation mit einem Dienst in der Umgebung, OE.NK.Zeitsynchro). Die Schlüssel für die VPN-Authentisierung liegen im sicheren Schlüsselspeicher (OE.NK.KeyStorage). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im

Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der beim VPN-Kanal genutzten kryptographischen Algorithmen und Protokollen richten.

4.3.2.3. T.NK.remote_EVG_LAN

Angriffe aus dem Transportnetz werden durch die VPN-Tunnel und den Paketfilter mit Stateful Packet Inspection (zustandsgesteuerte Filterung) abgewehrt: Anfragen, die ein Angreifer aus dem Transportnetz durch einen VPN-Tunnel zu senden versucht, werden vom EVG als ungültig erkannt (weil der Angreifer die VPN-Schlüssel nicht kennt, O.NK.VPN_Integrität) und verworfen. Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die Inhalte, die durch den VPN-Tunnel mit der zentralen TI-Plattform übertragen werden, sind nicht bösartig (OE.NK.sichere_TI). Anfragen außerhalb des VPN-Tunnels werden durch den dynamischen Paketfilter gefiltert (O.NK.PF_WAN); der EVG schützt durch diesen WAN-seitigen Paketfilter sich selbst und weitere dezentrale Komponenten im LAN der Leistungserbringer. Der WAN-seitige Paketfilter bietet zustandsgesteuerte Filterung (stateful packet inspection, zustandsgesteuerte Filterung, O.NK.Stateful). Der dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) protokolliert werden. Konnte ein Clientsystem bereits kompromittiert werden, so unterstützt auch der LAN-seitige Paketfilter beim Schutz des EVG (O.NK.PF_LAN): Im Fall einer Einbox-Lösung schützt der EVG (O.NK.PF_LAN) auch den Anwendungskonnektor vor LAN-seitigen Angriffen und trägt somit zur Abwehr der Bedrohung bei. Der EVG wird – wie bei T.NK.remote_EVG_WAN – unterstützt von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

Mit den gleichen Argumenten wie bei T.NK.remote_EVG_WAN (der Aufbau des sicheren Kanals wird vorab durch eine gegenseitige Authentisierung geschützt, die wiederum eine Zertifikatsgültigkeitsprüfung und eine Überprüfung der Systemzeit umfasst), tragen auch die Ziele O.NK.VPN_Auth, O.NK.Zert_Prüf, OE.NK.PKI, O.NK.Zeitdienst, OE.NK.Zeitsynchro, OE.NK.KeyStorage, OE.NK.Ersatzverfahren und OE.NK.RNG zur Abwehr der Bedrohung bei.

Angriffe aus dem Internet über den VPN-Tunnel vom Sicheren Internet Service (siehe Angriffspfad 3.2 in Abbildung 5) werden durch die Sicherheitsfunktionalität des Sicheren Internet Service verhindert (OE.NK.SIS). Entsprechende Zugriffe werden dadurch erkannt und vor der Weiterleitung über den VPN-Tunnel zum EVG blockiert. Zusätzlich kann der LAN-seitige Paketfilter (O.NK.PF_LAN) zum Schutz des LAN und des EVG beitragen. Konnte ein LAN dennoch kompromittiert werden, schützen die LAN-seitig installierten Maßnahmen zur Erkennung und Schutz vor bösartigem Code (OE.NK.Betrieb_CS) die Clientsysteme und den EVG.

4.3.2.4. T.NK.remote_VPN_Data

Der VPN-Client verschlüsselt die Daten mit einem starken kryptographischen Algorithmus; der Angreifer kann daher ohne Kenntnis der Schlüssel die verschlüsselte Nachricht nicht

entschlüsseln (O.NK.VPN_Vertraul). Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Dass die VPN-Schlüssel auf Seiten der VPN-Konzentratoren geheim gehalten werden, dafür sorgen OE.NK.sichere_TI und OE.NK.SIS. Dass die richtigen Daten auch tatsächlich verschlüsselt werden, dafür sorgt OE.NK.AK, indem zu schützende Daten der TI *und der Bestandsnetze* vom Anwendungskonnektor für den EVG erkennbar gemacht werden, unterstützt von OE.NK.Betrieb_AK (sicherer Betrieb des Anwendungskonnektors) und OE.NK.Betrieb_CS (sicherer Betrieb der Clientsysteme). Der VPN-Client vollzieht die Entschlüsselung von Daten, die ihm ein VPN-Konzentrator verschlüsselt zugesendet hat. Die Nutzdaten werden beim Senden integritätsgeschützt übertragen und beim Empfang auf ihre Integrität hin überprüft (O.NK.VPN_Integrität), was Manipulationen ausschließt.

Mit den gleichen Argumenten wie bei T.NK.remote_EVG_WAN (der Aufbau des sicheren Kanals wird vorab durch eine gegenseitige Authentisierung geschützt, die wiederum eine Zertifikatsgültigkeitsprüfung und eine Überprüfung der Systemzeit umfasst), tragen auch die Ziele O.NK.VPN_Auth, O.NK.Zert_Prüf, OE.NK.PKI, O.NK.Zeitdienst, OE.NK.Zeitsynchro, OE.NK.KeyStorage, OE.NK.Ersatzverfahren und OE.NK.RNG zur Abwehr der Bedrohung bei.

Anwendungshinweis 58: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

4.3.2.5. T.NK.local_admin_LAN

T.NK.local_admin_LAN betrachtet Angriffe im Zusammenhang mit lokaler Administration des EVG. Der EVG muss dazu eine Zugriffskontrolle implementieren (O.NK.Admin_EVG), so dass Administration nur durch Administratoren nach erfolgreicher Authentisierung (O.NK.Admin_Auth) möglich ist. Die Administratoren halten dazu ihre Authentisierungsinformationen geheim (OE.NK.Admin_EVG) und verhindern so, dass sich ein Angreifer dem EVG gegenüber als Administrator ausgeben kann. Dies wehrt bereits wesentliche Teile des beschriebenen Angriffs ab. Weitere Teilaspekte des Angriffs, insbesondere der Zugriff auf Schlüssel, werden durch weitere Ziele verhindert: Der Zugriff auf kryptographische Schlüssel und andere Geheimnisse im Arbeitsspeicher des EVGs wird durch entsprechende Speicheraufbereitung verhindert (aktives Löschen nach Verwendung der Geheimnisse, O.NK.Schutz). Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage. Administrative Tätigkeiten können im Sicherheits-Log mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) nachvollzogen werden (O.NK.Protokoll). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können.

Anwendungshinweis 59: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

4.3.2.6. T.NK.remote_admin_WAN

T.NK.remote_admin_WAN betrachtet Angriffe im Zusammenhang mit zentraler Administration. Der Unterschied im Angriffspfad zwischen T.NK.remote_admin_WAN und T.NK.local_admin_LAN besteht darin, dass der Angreifer bei T.NK.remote_admin_WAN aus

dem Transportnetz heraus versucht, seinen Angriff durchzuführen, während bei T.NK.local_admin_LAN die Angriffsversuche aus dem lokalen Netz heraus durchgeführt werden. Bei der Abwehr sind jedoch die gleichen Mechanismen beteiligt (Zugriffskontrolle, Authentisierung des Administrators, Selbstschutz, Protokollierung) und diese wirken unabhängig vom Ursprungsort des Angriffsversuchs, daher gilt hier sinngemäß das gleiche wie unter T.NK.local_admin_LAN: Zur Abwehr tragen die Ziele O.NK.Admin_EVG, O.NK.Admin_Auth, OE.NK.Admin_EVG, OE.NK.RNG, O.NK.Protokoll, O.NK.Schutz und OE.NK.KeyStorage bei.

4.3.2.7. T.NK.counterfeit

Bei der Bedrohung T.NK.counterfeit bringt ein Angreifer unbemerkt gefälschte Konnektoren in Umlauf. Neben der durch die Vertrauenswürdigkeitskomponente ALC_DEL.1 geforderten Überprüfung des Auslieferungsverfahrens und entsprechenden Verfahren zur Inbetriebnahme (AGD_OPE.1) ermöglicht der EVG auf Anforderung einen Nachweis seiner Authentizität (O.NK.EVG_Authenticity), der durch die kryptographische Identität im Sicherheitsmodul gSMC-K unterstützt wird (OE.NK.gSMC-K). Der EVG wird an einem zutrittsgeschützten Ort aufbewahrt (OE.NK.phys_Schutz), wodurch ein Entwenden erschwert wird. Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr aller Angriffe, die sich gegen Schwächen in kryptographischen Algorithmen und Protokollen richten, also auch bei Schwächen, die sich auf die kryptographische Identität beziehen.

4.3.2.8. T.NK.Zert_Prüf

Bei der Bedrohung T.NK.Zert_Prüf manipuliert ein Angreifer Sperrlisten, die zum Zwecke der Gültigkeitsprüfung von Zertifikaten von einem netzbasierten Dienst verteilt werden. Dieser Angriff wird durch das Ziel O.NK.Zert_Prüf auf Basis der über OE.NK.PKI erhaltenen Informationen abgewehrt. Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der bei den Zertifikaten genutzten kryptographischen Algorithmen richten.

Anwendungshinweis 60: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

4.3.2.9. T.NK.TimeSync

T.NK.TimeSync beschreibt den Angriff, dass Nachrichten manipuliert werden, die im Rahmen einer Zeitsynchronisation mit einem netzbasierten Dienst ausgetauscht werden, um auf dem EVG die Einstellung einer falschen Echtzeit zu bewirken. Dieser Angriff wird durch das Ziel O.NK.Zeitdienst abgewehrt, da dieses die Synchronisation der durch die Umgebung bereitgestellte Echtzeituhr (OE.NK.Echtzeituhr) über einen sicheren Kanal fordert. Weil der Zeitdienst innerhalb der zentralen Telematikinfrastruktur-Plattform bereitgestellt wird, dient bereits der VPN-Tunnel zu dem VPN-Konzentrator für den Zugang zur Telematikinfrastruktur als sicherer Kanal (O.NK.VPN_Integrität). Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Beim Aufbau des Kanals werden die Kummunikationspartner authentisiert (O.NK.VPN_Auth) und Zertifikat geprüft (O.NK.Zert_Prüf) gegen die PKI der TI (OE.NK.PKI). Sichere Ersatzverfahren

(OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der beim VPN-Kanal genutzten kryptographischen Algorithmen richten. Die Zeitserver, die über eine verlässliche Systemzeit verfügen und somit die Basis für eine vertrauenswürdige Zeitinformation im Rahmen der Synchronisierung bilden, werden durch die Umgebung bereitgestellt (OE.NK.Zeitsynchro); außerdem liegen sie innerhalb der Telematikinfrastruktur und bilden somit die Gegenseite des sicheren Kanals.

Anwendungshinweis 61: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

4.3.2.10. T.NK.DNS

Die Bedrohung T.NK.DNS beschreibt einen Angriff aus dem Transportnetz, bei dem Antworten auf DNS-Anfragen gefälscht werden. Solche DNS-Anfragen an DNS-Server im Transportnetz bzw. im Internet kommen nur in solchen Szenarien vor, bei denen Adressen im Transportnetz bzw. Internet aufgelöst werden sollen[24]. Der Netzkonnektor löst die öffentlichen Adressen der VPN-Konzentratoren mittels DNS-Anfragen auf. Bei erfolgtem Angriff bekommt er nicht die gewünschte Adresse zurück. Das führt aber dazu, dass er keinen VPN-Kanal aufbauen kann, da durch das Sicherheitsziel O.NK.VPN_Auth die Authentisierung der VPN-Konzentratoren erforderlich ist. Dabei findet eine Zertifikatsprüfung statt (O.NK.Zert_Prüf) gegen die PKI der TI (OE.NK.PKI). Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der bei den Zertifikaten genutzten kryptographischen Algorithmen richten. Damit erlangt der Angreifer keinen Zugriff auf das LAN des Leistungserbringers und kann die zu schützenden Daten nicht angreifen. Bei versuchtem Angriff kann dieser unter Umständen durch den Paketfilter des Netzkonnektors erkannt und verhindert werden (O.NK.PF_WAN, O.NK.Stateful). Dies hängt einerseits vom Vorgehen des Angreifers und andererseits von der Funktionalität des Paketfilters ab. Bei erkanntem Angriff erfolgt ferner ein Eintrag mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) in das Sicherheitsprotokoll (O.NK.Protokoll).

Im Fall einer DNS-Auflösung durch Clientsysteme beim Zugriff auf das Internet führt die Manipulation der DNS-Antwort dazu, dass Clientsysteme auf Seiten umgelenkt werden können, die nicht ihrer ursprünglichen Intention entsprechen. Erfolgt dies vom Benutzer unbemerkt, können bei bösartigen Systemen die Clientsysteme durch bösartigen Code infiziert werden. Dies kann teilweise durch Erkennungsmechanismen im SIS verhindert werden, welches wirksame Maßnahmen gegen Angriffe aus dem Internet implementieren soll (OE.NK.SIS). In jedem Fall muss der bösartige Code auf den Clientsystemen aber durch Mechanismen auf den Clientsystemen (Einsatz von sicheren Produkten und Virenscannern) erkannt und neutralisiert werden (OE.NK.Betrieb_CS).

[24] Für Namensauflösungen innerhalb der TI und der darin angeschlossenen Netzwerke stellt die TI eigene DNS-Server bereit, die vom Transportnetz bzw. Internet nicht erreichbar sind.

4.3.3. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

4.3.3.1. OSP.NK.Zeitdienst

Die organisatorische Sicherheitspolitik OSP.NK.Zeitdienst fordert einen Zeitdienst sowie eine regelmäßige Zeitsynchronisation mit Zeitservern.

Die regelmäßige Zeitsynchronisation wird durch O.NK.Zeitdienst gefordert. Die Echtzeituhr, welche im Rahmen der Zeitsynchronisation synchronisiert wird, wird durch die Umgebung (OE.NK.Echtzeituhr) bereitgestellt; ohne die Echtzeituhr gäbe es kein Ziel für die im Rahmen der Zeitsynchronisation ausgetauschten Zeitinformationen und der EVG könnte keinen Zeitdienst anbieten, daher unterstützt dieses Umgebungsziel ebenfalls die OSP.NK.Zeitdienst. Damit die Zeitsynchronisation stattfinden kann und im Rahmen der Synchronisation die korrekte Zeit ausgetauscht wird, bedarf es einer Menge von Zeitservern, welche über eine verlässliche Systemzeit verfügen; diese Zeitserver werden durch die Umgebung bereitgestellt (OE.NK.Zeitsynchro).

4.3.3.2. OSP.NK.SIS

Die Sicherheitspolitik OSP.NK.SIS fordert einen gesicherten Internet-Zugangspunkt, der die damit verbundenen Netze der Benutzer wirksam gegen Angriffe aus dem Internet schützt. Dieser Zugang wird durch O.NK.PF_WAN (mit zustandsgesteuerter Filterung, O.NK.Stateful) ermöglicht. Von diesem System dürfen keine Angriffe auf die Netze der Benutzer ausgehen.

Genau diese Eigenschaften werden durch OE.NK.SIS gefordert. Das schließt neben den technischen Schutzmaßnahmen auch eine sichere Administration des Zugangspunktes ein.

4.3.3.3. OSP.NK.BOF

Die Sicherheitspolitik OSP.NK.BOF fordert eine Kommunikation der aktiven Komponenten des LAN des LE mit den Bestandsnetzen und offenen Fachdiensten über den VPN-Kanal zur TI. Diese Kommunikation wird durch den VPN-Kanal entsprechend O.NK.PF_WAN, O.NK.VPN_Integrität, O.NK.VPN_Vertraul, O.NK.Zert_Prüf und durch den Paketfilter nach O.NK.PF_WAN (mit zustandsgesteuerter Filterung, O.NK.Stateful) ermöglicht und kontrolliert. Gemäß OE.NK.CS erfolgt der Zugriff auf Bestandsnetze und offene Fachanwendungen nur durch aktive Komponenten im LAN in den vorgesehenen IP-Adressbereichen.

4.3.3.4. OSP.NK.TLS

Die Sicherheitspolitik OSP.NK.TLS fordert die Bereitstellung von TLS-Kanälen unter Verwendung sicherer kryptographischer Algorithmen und Protokolle zur sicheren Kommunikation mit anderen IT-Produkten. Diese TLS-Kanäle werden durch O.NK.TLS_Krypto ermöglicht.

4.3.3.5. OSP.NK.SW-Update

Die Sicherheitspolitik OSP.NK.SW-Update erlaubt das Einspielen von Software für Konnektorkomponenten im Sinne einer Aktualisierung sowie das Aktualisieren der TSF Daten

und das Nachladen von Fachmodulen. Dies ist ein administrativer Vorgang und damit auf Personen mit administrativen Zugriffsrechten beschränkt. Dies wird durch das Sicherheitsziel O.NK.Admin_EVG erreicht. In diesem Zusammenhang stehende sicherheitsrelevante Ereignisse werden durch O.NK.Protokoll protokolliert und mit einem sicheren Zeitstempel versehen. Bei der Bereitstellung der Update-Daten sorgt die Einsatzumgebung gemäß OE.NK.SW-Update dafür, dass nur geprüfte und von einer autorisierten Stelle freigegebene SW-Updates signiert und ausgeliefert werden. Ebenso sorgt OE.NK.SW-Update dafür, dass nur geprüfte und von einer autorisierten Stelle freigegebene Fachmodule signiert und ausgeliefert werden. Zum Software-Update im EVG fordert O.NK.Update, dass nur solche Updates eingespielt werden dürfen, deren Integrität und Authentizität gesichert ist.

4.3.4. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Bei den inhaltlich lediglich umformulierten Annahmen (A. ...) bzw. Umgebungszielen (OE. ...) besteht eine direkte Eins-zu-eins-Beziehung: A.NK.phys_Schutz, A.NK.gSMC-K, A.NK.sichere_TI, A.NK.kein_DoS, A.NK.AK, A.NK.CS, A.NK.Betrieb_AK, A.NK.Betrieb_CS, A.NK.Admin_EVG und A.NK.Ersatzverfahren lassen sich direkt den entsprechend bezeichneten Umgebungszielen zuordnen: OE.NK.phys_Schutz, OE.NK.gSMC-K, OE.NK.sichere_TI, OE.NK.kein_DoS, OE.NK.AK, OE.NK.CS, OE.NK.Betrieb_AK, OE.NK.Betrieb_CS, OE.NK.Admin_EVG und OE.NK.Ersatzverfahren. Zu jeder dieser Annahmen existiert ein entsprechendes Umgebungsziel.

Die Annahme A.NK.Zugriff_gSMC-K lautet:

> *Es sind effektive Zugriffsschutzmaßnahmen etabliert, die den möglichen Zugriff von Komponenten des Konnektors auf Schlüsselmaterial der gSMC-K kontrollieren und unzulässige Zugriffe verhindern. Die Zugriffskontrolle kann durch eine zentrale Instanz vermittelt werden oder es wird sichergestellt, dass die Komponenten des Konnektors nur auf ihr eigenes Schlüsselmaterial zugreifen.*

Diese Annahme wird wie folgt auf die Umgebungsziele OE.NK.gSMC-K und OE.NK.Betrieb_AK abgebildet:

OE.NK.gSMC-K impliziert, dass eine gSMC-K existiert und von der gematik zugelassen ist, und dass der EVG Zugriff auf dieses Modul hat. Der Hersteller des EVG verbaut nur solche zugelassenen Module und die gSMC-K ist sicher mit dem EVG verbunden, so dass die Kommunikation zwischen gSMC-K und EVG weder mitgelesen noch manipuliert werden kann. Somit müssen im Rahmen der Zugriffskontrolle überhaupt nur Zugriffe anderer Konnektorteile (AK) auf die gSMC-K betrachtet werden.

Laut OE.NK.Betrieb_AK trägt der Betreiber des EVG die Verantwortung dafür, dass die Anwendungskonnektoren und Fachmodule den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen. Im Rahmen dieser Betrachtung wird das Vorhandensein einer wirksamen Zugriffskontrolle im Gesamtkonnektor sichergestellt.

5. Definition zusätzlicher Komponenten

5.1. Definition der erweiterten Familie FPT_EMS und der Anforderung FPT_EMS.1

Die Definition der Familie FPT_EMS wurde aus dem Card Operating System (PP COS) [10], Abschnitt 6.6.1 übernommen.

Family **FPT_EMS – EVG Emanation**

Family behaviour This family defines requirements to mitigate intelligible emanations.

Component levelling: **FPT_EMS – EVG Emanation** — 1

FPT_EMS.1 – EVG Emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit:FPT_EMS.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FPT_EMS.1 **Emanation of TSF and User data**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6. Sicherheitsanforderungen

6.1.1. Hinweise zur Notation

Die Auswahl der funktionalen Sicherheitsanforderungen ist durch das zugrundeliegende Schutzprofil, BSI-CC-PP-0097-V2-2020-MA-02, gegeben. Das Schutzprofil basiert auf Version 3.1 Revision 5 der Common Criteria. Dieses Security Target basiert ebenfalls auf der aktuelleren Version 3.1 Revision 5 der Common Criteria und übernimmt die Formulierungen des Schutzprofils.

Die Common Criteria erlauben die Anwendung verschiedener Operationen auf die funktionalen Sicherheitsanforderungen; *Verfeinerung, Auswahl, Zuweisung und Iteration*. Jede dieser Operationen wird in diesem Security Target angewandt.

Die Operation **Verfeinerung** (refinement) wird genutzt, um Details zu einer Anforderung hinzuzufügen und schränkt diese Anforderung folglich weiter ein. In diesem Security Target werden Verfeinerungen durch **fettgedruckten Text** in der Anforderung hervorgehoben bzw. mit einer entsprechenden Fußnote gekennzeichnet oder sie werden der Anforderung in einem mit dem Wort „Refinement:“ eingeleiteten Absatz hinzugefügt. Gegebenenfalls werden sie in einem der Anforderung folgenden Anwendungshinweis näher erläutert. Gelöschter Text wird **~~fettgedruckt und durchgestrichen~~** dargestellt.

Die Operation **Auswahl** (selection) wird genutzt, um eine oder mehrere durch die CC vorgegebenen Optionen auszuwählen. In diesem Security Target wird eine bereits im PP ausgeführte Auswahl durch unterstrichenen Text in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben. Eine durch das PP bzw. CC Teil 2 [2] vorgegebene und im Security Target ausgeführte Auswahl wird zusätzlich durch [eckige Klammern] hervorgehoben.

Die Operation **Zuweisung** (assignment) wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Security Target werden bereits im PP ausgeführte Zuweisungen durch *kursiven Text* in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben. Durch das PP bzw. CC Teil 2 [2]vorgegebene und im Security Target ausgeführte Zuweisungen werden zusätzlich durch [*eckige Klammern*] hervorgehoben.

Die Operation **Iteration** wird genutzt, um eine Komponente mit unterschiedlichen Operationen zu wiederholen. In diesem Security Target werden Iterationen durch einen Schrägstrich „/“ und den Iterationsidentifikator hinter dem Komponentenidentifikator angegeben.

6.2. Funktionale EVG-Sicherheitsanforderungen

Die funktionalen Sicherheitsanforderungen werden im Folgenden nicht wie sonst häufig in alphabetischer Reihenfolge aufgezählt, sondern nach funktionalen Gruppen gegliedert. Dadurch soll ein besseres Verständnis der Anforderungen und ihrer Abhängigkeiten

untereinander erreicht werden. Die funktionalen Gruppen orientieren sich an den in Abschnitt 1.3.5 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

- VPN-Client: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);
- Dynamischer Paketfilter: sowohl für WAN als auch für LAN;
- Netzdienste: Zeitsynchronisation über sicheren Kanal, Zertifikatsprüfung mittels Sperrlisten;
- Stateful Packet Inspection: Generierung von Audit-Daten für spätere zustandsgesteuerte Filterung;
- Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, optional sichere Kanäle zu anderen Komponenten des Konnektors, Protokollierung Sicherheits-Log;
- Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, eingeschränkte Möglichkeit der Administration von Firewall-Regeln;
- Kryptographische Basisdienste
- Nutzung starker kryptographischer Verfahren für TLS-Verbindungen.

Um die Semantik von Sicherheitsanforderungen leichter erkennen zu können, wurden den Anforderungen teilweise **Suffixe** angehängt, z. B. „/NK.VPN_TI“ für den Trusted Channel, der den VPN-Kanal in die Telematikinfrastruktur fordert (siehe FTP_ITC.1/NK.VPN_TI). Diese Vorgehensweise erleichtert es auch, inhaltlich zusammenhängende Anforderungen zu identifizieren (z. B. FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF und FMT_MSA.3/NK.PF) und iterierte Komponenten zu unterscheiden. Für alle SFRs aus diesem Security Target wurde zudem das Suffix „NK“ verwendet, selbst wenn keine Iteration vorliegt. Das wurde zur Vereinfachung im Umgang mit der vorgesehenen Evaluierung des Gesamt-Konnektors eingeführt, bei der die in diesem Schutzprofil definierten SFRs wiederverwendet werden sollen.

6.2.1. VPN-Client

VPN

Um die Sicherheitsanforderungen, die wesentlich durch den VPN-Client für die Telematikinfrastruktur bedingt werden, leicht erkennen zu können, wurden diese Sicherheitsanforderungen durch das Suffix „/VPN_TI“ gekennzeichnet. Analog dazu werden Sicherheitsanforderungen, die wesentlich durch den VPN-Client des Sicheren Internet Service bedingt werden, durch das Suffix „/VPN_SIS“ gekennzeichnet.

FTP_ITC.1/NK.VPN_TI Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_TI The TSF shall provide a communication channel between itself and another trusted IT product **VPN-Konzentrator der**

Telematikinfrastruktur[25] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[26] and protection of the channel data from modification **and**[27] disclosure.

FTP_ITC.1.2/NK.VPN_TI The TSF shall permit the TSF[28] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_TI The TSF shall initiate communication via the trusted channel for *communication with the TI*[29].

Refinement: Die Anforderung „protection of the channel data from modification and disclosure“ in FTP_ITC.1.1/NK.VPN_TI ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Der Trusted Channel muss auf Basis des **IPsec**-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [16], RFC 4301 (IPsec) [27], RFC 4303 (ESP) [30]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [31]) unterstützt werden.

Die Anforderung „assured identification” in FTP_ITC.1.1/NK.VPN_TI impliziert, dass der EVG die Authentizität des VPN-Konzentrators überprüfen muss. Im Rahmen dieser Überprüfung muss er eine Zertifikatsprüfung durchführen (siehe FPT_TDC.1/NK.Zert).

Erläuterung: Die von O.NK.VPN_Auth geforderte gegenseitige Authentisierung der Endpunkte wird durch FTP_ITC.1.1/NK.VPN_TI geleistet (assured identification of its end points).

Der von O.NK.VPN_Vertraul und O.NK.VPN_Integrität geforderte Schutz der Vertraulichkeit und Datenintegrität der Nutzdaten wird ebenfalls durch FTP_ITC.1.1/NK.VPN_TI geleistet (protection of the channel data from modification *and* disclosure). Um beide Aspekte verbindlich zu machen, wurde die Verfeinerung (refinement) von *or* zu *and* durchgeführt.

FTP_ITC.1/NK.VPN_SIS Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_SIS The TSF shall provide a communication channel between itself and another trusted IT product **Sicherer Internet Service (SIS)**[30] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate**

---

25 refinement

26 refinement

27 refinement (or → and)

28 [selection: *the TSF, another trusted IT product*]

29 [assignment: *list of functions for which a trusted channel is required*]

30 refinement

based authentication[31] and protection of the channel data from modification **and**[32] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[33] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_SIS The TSF shall initiate communication via the trusted channel for all *communication with the SIS*[34].

Refinement: Die Anforderung „protection of the channel data from modification and disclosure“ in FTP_ITC.1.1/NK.VPN_SIS ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten) aller Kommunikation mit dem Internet. Der Trusted Channel muss auf Basis des **IPsec**-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [16], RFC 4301 (IPsec) [27], RFC 4303 (ESP) [30]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [31]) unterstützt werden.

Die Anforderung „assured identification” in FTP_ITC.1.1/NK.VPN_SIS impliziert, dass der EVG die Authentizität des VPN-Konzentrators überprüfen muss. Im Rahmen dieser Überprüfung muss er eine Zertifikatsprüfung durchführen (siehe FPT_TDC.1/NK.Zert).

Erläuterung: Die von O.NK.VPN_Auth geforderte gegenseitige Authentisierung der Endpunkte wird durch FTP_ITC.1.1/NK.VPN_SIS geleistet (assured identification of its end points).

Der von O.NK.VPN_Vertraul und O.NK.VPN_Integrität geforderte Schutz der Vertraulichkeit und Datenintegrität der Nutzdaten wird ebenfalls durch FTP_ITC.1.1/NK.VPN_SIS geleistet (protection of the channel data from modification *and* disclosure). Um beide Aspekte verbindlich zu machen, wurde die Verfeinerung (refinement) von *or* zu *and* durchgeführt.

Anwendungshinweis 62: Der EVG unterstützt RFC 7296 (IKEv2) [31], siehe [18], Kapitel 3.3.1. Dieser Hinweis bezieht sich auf FTP_ITC.1.1/NK.VPN_SIS und FTP_ITC.1.1/NK.VPN_TI.

Anwendungshinweis 63: Eine theoretisch mögliche Kommunikation von EVGs untereinander wird in diesem Security Target nicht behandelt.

---

31 refinement

32 refinement (or → and)

33 [selection: *the TSF, another trusted IT product*]

34 [assignment: *list of functions for which a trusted channel is required*]

Informationsflusskontrolle

Die Informationsflusskontrolle ergibt sich zwar aus der Betrachtung der VPN-Kanäle (aufgrund der Frage: Wie wird der Eingang in den VPN-Tunnel geschützt?), sie wird aber im Hinblick auf ihre Realisierung der Anforderung nach Informationsflusskontrolle mittels einem dynamischen Paketfilter (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, siehe unten in Abschnitt 6.2.2) zugeordnet; das „PF“ steht dabei für Paketfilter. Daher finden sich die Anforderungen (SFR) zu diesen Aspekten im nächsten Abschnitt 6.2.2.

Die von O.NK.PF_WAN und O.NK.PF_LAN erzwungene VPN-Nutzung für *zu schützende Daten der TI und der Bestandsnetze* und für *zu schützende Nutzerdaten* (im Sinne des Abschnitts 3.1) wird durch FDP_IFF.1.2/NK.PF umgesetzt, sofern die Paketfilter-Regeln geeignet gesetzt sind, was wiederum durch die Administratordokumentation (siehe das Refinement zu AGD_OPE.1 in Abschnitt 6.3.2) sichergestellt wird.

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Alle funktionalen Anforderungen, die mit dem Paketfilter in direktem Zusammenhang stehen, wurden mit dem Suffix „/NK.PF“ (wie Paketfilter) versehen.

Dynamischer Paketfilter

FDP_IFC.1/NK.PF Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

hier erfüllt durch: FDP_IFF.1/NK.PF

FDP_IFC.1.1/ NK.PF The TSF shall enforce the *packet filtering SFP (PF SFP)*[35] on the *subjects*

(1) IAG,

(2) VPN concentrator of the TI,

(3) VPN concentrator of the SIS,

(4) the TI services ,

(5) application connector (except the service modules),

(6) the service modules (German: Fachmodule) running on the application connector,

(7) active entity in the LAN,

(8) CRL download server,

(9) hash&URL server,

(10) registration server of the VPN network provider,

[35] [assignment: *information flow control SFP*]

(11) remote management server,

the information

(1) incoming information flows

(2) outgoing information flows

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[36].

Anwendungshinweis 64: Die dynamischen Paketfilter (LAN-seitig und WAN-seitig) sollen sowohl den EVG vor Angriffen bzw. vor unerlaubten Informationsflüssen (i) aus dem LAN und (iii) aus dem WAN schützen als auch die Informationsflüsse zwischen (ii) LAN und WAN bzw. (iv) zwischen WAN und LAN kontrollieren.

Anwendungshinweis 65: Systembedingt bietet IPv4 (Internet Protocol, Version 4) nur eine Identifikation der Informationsflüsse, aber keine Authentisierung. Aus Mangel an besseren Mechanismen müssen dennoch auf dieser Basis die Entscheidungen über die Zulässigkeit von Informationsflüssen getroffen werden.

Für die Beschreibung der Filterregeln werden folgende IP-Adressbereiche definiert:

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der WAN-Adapter des Konnektors angeschlossen ist.
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der LAN-Adapter des Konnektors angeschlossen ist.
ANLW_LEKTR_INTRANET_ROUTES	Adressbereich des Intranet-VPN des LE
NET_SIS	VPN-Konzentratoren der SIS
NET_TI_ZENTRAL	Zentrale Dienste der TI
NET_TI_DEZENTRAL	Adressbereich der WAN-Schnittstellen der Konnektoren für die Kommunikation mit der TI oder den Bestandsnetzen
NET_TI_OFFENE_FD	Offene Fachdienste der TI
NET_TI_GESICHERTE_FD	Gesicherte Fachdienste der TI

[36] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_BESTANDSNETZE	die an die TI angeschlossenen Bestandsnetze
ANLW_AKTIVE_BESTANDSNETZE	die an die TI angeschlossenen und vom Administrator freigeschalteten Bestandsnetze
VPN_KONZENTRATOR_TI_IP_ADDRESS	IP-Adresse des VPN-Konzentrators der TI
VPN_KONZENTRATOR_SIS_IP_ADDRESS	IP-Adresse des VPN-Konzentrators des SIS
DNS_SERVERS_BESTANDSNETZE	IP-Adressen von DNS-Servern für die Bestandsnetze (ANLW_BESTANDSNETZE)
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
DNS_ROOT_ANCHOR_URL	IP-Adresse des DNSSEC Vertrauensankers für das Internet
hash&URL-Server	IP-Adresse des hash&URL-Servers
registration server	IP-Adresse des Registrierungsservers
remote management server	IP-Adresse des Remote-Managementservers
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.
TSL_DOWNLOAD_ADDRESS	IP-Adresse des TSL-Download-Punktes des TSL-Dienstes.

IP-Adressen des Konnektors	Erläuterung
ANLW_LAN_IP_ADDRESS	LAN-seitige Adresse des EVG, unter dieser Adresse werden die Dienste des Konnektor im lokalen Netzwerk bereitgestellt werden.
ANLW_WAN_IP_ADDRESS	WAN-seitige Adresse des EVG
VPN_TUNNEL_TI_INNER_IP	IP-Adresse des Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren der TI
VPN_TUNNEL_SIS_INNER_IP	IP-Adresse des Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren des SIS

Für die Beschreibung der Filterregeln werden folgende Konfigurationsparameter des EVG definiert:

Konfigurationsparameter	Bedeutung und [Werte]

ANLW_WAN_ADAPTER_MODUS	Parameter aktiviert [ENABLED] oder deaktiviert [DISABLED] den WAN-Port des EVG
ANLW_ANBINDUNGS_MODUS	Parameter beschreibt die Art der Anbindung des EVGs in das LAN des Nutzers. Bei Schaltung [InReihe] befindet sich der EVG als erste Komponente hinter dem IAG und das LAN spannt sich hinter dem EVG auf. Wenn ANLW_WAN_ADAPTER_MODUS=ENABLED befindet sich der EVG in dieser Schaltung. Bei Schaltung [Parallel] befindet sich der EVG als eine von weiteren Komponenten im LAN. Wenn ANLW_WAN_ADAPTER_MODUS=DISABLED befindet sich der EVG in dieser Schaltung.
MGM_LOGICAL_SEPARATION	Parameter aktiviert [Enabled] oder deaktiviert [Disabled] die logische Trennung, wodurch trotz Verbindung des EVG mit dem IAG und darüber mit TI Services eine Verbindung von Clientsystemen mit dem Internet, TI Services und Bestandsnetzen vom EVG unterbunden wird.
ANLW_INTERNET_MODUS	Parameter regelt das Routing von Paketen von Clientsystemen im LAN mit dem Ziele im Bereich Internet. Bei Konfiguration [KEINER] wird kein Traffic ins Internet geroutet. Bei Konfiguration [SIS] wird Internet-Traffic aus dem LAN über den VPN-Tunnel zum SIS geroutet. Bei Konfiguration [IAG] wird das Clientsystem per ICMP-Redirect auf die Route zum IAG verwiesen.
ANLW_FW_SIS_ADMIN_RULES	Hierbei handelt es sich um vom Administrator definierte Firewall-Regeln (zusätzlich zu den hier beschriebenen) für den einschränkenden Zugriff auf den SIS. Werte sind hier Regeln mit den Parametern Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll (ggf. mit Absender-Port und Empfänger-Port) und Verbindungsrichtung.

FDP_IFF.1/NK.PF Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_MSA.3 Static attribute initialisation

hier erfüllt durch: FMT_MSA.3/NK.PF (restriktive Filterregeln)

FDP_IFF.1.1/NK.PF The TSF shall enforce the *PF SFP*[37] based on the following types of subject and information security attributes:

For all subjects and information as specified in FDP_IFC.1/NK.PF, the decision shall be based on the following security attributes:

(1) IP address,

(2) port number,

(3) protocol type,

(4) *direction (inbound and outbound IP*[38] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES. [39]

FDP_IFF.1.2/NK.PF The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

(1) For every operation receiving or sending data the TOE shall maintain a set of packet filtering rules that specifies the allowed operations by (i) direction (inbound or outbound), (ii) source and destination IP address involved, and (iii) source and destination port numbers involved in the information flow.

(2) The TSF is allowed to communicate with the IAG through the LAN interface if (ANLW_WAN_ADAPTER_MODUS = DISABLED).

(3) The TSF shall communicate with the IAG through the WAN interface if (ANLW_WAN_ADAPTER_MODUS = ACTIVE and ANLW_ANBINDUNGS_MODUS = InReihe).

(4) The connector using the IP address ANLW_WAN_IP_ADDRESS is allowed to communicate via IAG

a) by means of IPSEC protocol with VPN concentrator of TI with IP-Address VPN_KONZENTRATOR_TI_IP_ADDRESS,

b) by means of IPSEC protocol with VPN concentrator of SIS with IP-Address VPN_KONZENTRATOR_SIS_IP_ADDRESS,

---

37 [assignment: *information flow control SFP*]

38 IP = Internet Protocol

39 [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

c) *by means of protocols HTTP and HTTPS with IP-Address CERT_CRL_DOWNLOAD_ADDRESS, DNS_ROOT_ANCHOR_URL, hash&URL Server, registration server and remote management server,*

d) *by means of protocol HTTP with IP-Address TSL_DOWNLOAD_ADDRESS,*

e) *by means of protocol DNS to any destination.*

(5) *The active entities in the LAN with IP addresses within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES are allowed to communicate with the connector for access to base services.*

(6) *The application connector is allowed to communicate with active entities in the LAN.*

(7) *The TSF shall allow*

a) *to establish the IPsec tunnel with the VPN concentrator of TI if initiated by the application connector and*

b) *to send packets with destination IP address VPN_KONZENTRATOR_TI_IP_ADDRESS and to receive packets with source IP address VPN_KONZENTRATOR_TI_IP_ADDRESS in the outer header of the IPsec packets.*

(8) *The following rules based on the IP addresses in the inner header of the IPSec packet apply for the communication TI through the VPN tunnel between the connector and the VPN concentrator:*

a) *Communication is allowed between entities with IP address within NET_TI_ZENTRAL and application connector.*

b) *Communication is allowed between entities with IP address within NET_TI_GESICHERTE_FD and application connector.*

c) *If MGM_LU_ONLINE=Enabled the communication between entities with IP address within NET_TI_GESICHERTE_FD and by service moduls is allowed.*

d) *Communication between entities with IP address within NET_TI_OFFENE_FD and active entity in the LAN is allowed.*

e) *Communication between entities with IP address within NET_TI_OFFENE_FD and a service module is allowed.*

f) *If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled) the TSF shall allow communication of connector with DNS with IP address within DNS_SERVERS_BESTANDSNETZE.*

g) If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled) the TSF shall allow communication of active entities in the LAN with entities with IP address within ANLW_AKTIVE_BESTANDSNETZE.

(9) The TSF shall allow

a) to establish the IPsec tunnel with the SIS concentrator if initiated by the application connector and

b) to send packets with destination IP address VPN_KONZENTRATOR_SIS_IP_ADDRESS and to receive packets with source IP address VPN_KONZENTRATOR_SIS_IP_ADDRESS in the outer header of the IPsec packets..

(10) Packets with source IP address within NET_SIS shall be received with outer header of the VPN tunnel from the VPN concentrator of the SIS only.

(11) For the communication though the VPN tunnel with VPN concentrator of the SIS the following rules based on the IP addresses in the inner header of the IPSec packets apply:

a) If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=SIS) the application connector and active entities in the LAN are allowed to communicate through the VPN tunnel with the SIS.

b) The rules ANLW_FW_SIS_ADMIN_RULES applies if defined.

(12) The TSF shall redirect the packets received from active entities in the LAN to the default gateway if the packet destination address is not (NET_TI_ZENTRAL or NET_TI_OFFENE_FD or NET_TI_GESICHERTE_FD or ANLW_AKTIVE_BESTANDSNETZE) and if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=IAG).

(13) The TSF shall redirect communication from IAG to active entities in the LAN if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=IAG und ANLW_IAG_ADDRESS≠““).[40]

FDP_IFF.1.3/NK.PF The TSF shall enforce the following additional information flow control SFP rules:

[40] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

(1) The TSF shall enforce SFP rules ANLW_FW_SIS_ADMIN_RULES

(2) *The TSF shall transmit data (except for establishment of VPN connections) to the WAN only if the IPsec VPN tunnel between the TSF and the remote VPN concentrator has been successfully established and is active and working*[41].

FDP_IFF.1.4/NK.PF The TSF shall explicitly authorise an information flow based on the following rules*: Stateful Packet Inspection,* [*no additional rules*][42].

Refinement: Stateful Packet Inspection (zustandsgesteuerte Filterung) bedeutet in diesem Zusammenhang, dass der EVG zur Entscheidungsfindung, ob ein Informationsfluss zulässig ist oder nicht, nicht nur jedes einzelne Paket betrachtet, sondern auch den Status einer Verbindung mit in diese Entscheidung einbezieht.

FDP_IFF.1.5/NK.PF The TSF shall explicitly deny an information flow based on the following rules:

(1) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with NET_TI_GESICHERTE_FD, NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL outside VPN channel to VPN concentrator of the TI.

(2) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with SIS outside VPN channel to VPN concentrator of the SIS.

(3) The TSF prevents communication of active entities in the LAN with destination IP address within ANLW_AKTIVE_BESTANDSNETZE initiated by active entities in the LAN, if (MGM_LOGICAL_SEPARATION=Enabled).

(4) The TSF prevents communication of active entities in the LAN with entities with IP addresses within ANLW_BESTANDSNETZE but outside ANLW_AKTIVE_BESTANDSNETZE.

(5) The TSF prevents communication of service modules with NET_TI_ZENTRAL, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE and internet via SIS or IAG.

(6) The TSF prevents communication initiated by entities with IP address within NET_TI_GESICHERTE_FD, NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL (except the connector itself), ANLW_BESTANDSNETZE and NET_SIS.

---

41 [assignment: *additional information flow control SFP rules*]

42 [assignment: *rules, based on security attributes, that explicitly authorise information flow*]

(7) The TSF prevents communication of entities with IP addresses in the inner header within NET_TI_ZENTRAL, NET_TI_GESICHERTE_FD, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE, ANLW_LAN_ADDRESS_SEGMENT, ANLW_LEKTR_INTRANET_ROUTES and ANLW_WAN_NETWORK_SEGMENT coming through the VPN tunnel with VPN concentrator of the SIS.

(8) The TSF prevents receive of packets from entities in LAN if packet destination is internet and (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS = KEINER).

(9) The TSF prevents inbound packets of the VPN channels from SIS with destination address in the inner header outside
a) ANLW_LAN_IP_ADDRESS or
b) ANLW_LEKTR_INTRANET_ROUTES if ANLW_WAN_ADAPTER_MODUS=DISABLED or
c) ANLW_WAN_IP_ADDRESS if ANLW_WAN_ADAPTER_MODUS=ACTIVE

(10) The TSF prevents communication of IAG to connector through LAN interface if (ANLW_WAN_ADAPTER_MODUS= ACTIVE).

(11) The TSF prevents communication of IAG to connector through WAN interface of the connector if (ANLW_WAN_ADAPTER_MODUS= DISABLED).

(12) [*no additional rules*][43].

Refinement: Alle nicht durch den Paketfilter explizit erlaubten Informationsflüsse müssen verboten sein (default-deny).

Erläuterung: Der von O.NK.PF_WAN und O.NK.PF_LAN geforderte dynamische Paketfilter wird durch FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF gefordert.

Der Mechanismus „Logische Trennung“ (siehe [16], TIP1-A_4823) wird vom RISE-Konnektor V6.0 nicht implementiert. Für das Attribut MGM_LOGICAL_SEPARATION kann der Wert daher nicht auf ENABLED gesetzt werden.

[43] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

Anwendungshinweis 66: Durch die Festlegung verbindlicher, nicht administrierbarer Paketfilter-Regeln (vgl. auch das Refinement zu FMT_MSA.1/NK.PF) und bei Wahl eines geeigneten Satzes von Paketfilter-Regeln (siehe dazu das Refinement zu AGD_OPE.1 in Abschnitt 6.3) erzwingt FDP_IFF.1.2/NK.PF die VPN-Nutzung für zu schützende Daten der TI und der Bestandsnetze und zu schützende Nutzerdaten wie in Abschnitt 3.1 definiert.

Anwendungshinweis 67: Der EVG verwaltet Informationen über eine (kurze) Historie der Verbindung durch die Funktionalität des Betriebsystemkernels. Eingehende Verbindungen werden nur als Antworten auf zuvor ausgegangene Anfragen zugelassen, so dass ein ungefragter Verbindungsaufbau aus dem WAN wirkungsvoll verhindert wird. Siehe auch stateful packet inspection im Glossar.

Anwendungshinweis 68: Die dynamische Paketfilterung soll die Menge der zulässigen Protokolle im Rahmen der Kommunikation mit der Telematikinfrastruktur geeignet beschränken. Es sind nur die in der Spezifikation Netzwerk [gemSpec_Net] [17], Tabelle 1 aufgeführten Protokolle zulässig. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.

Entsprechend der Anforderungen an die in O.NK.PF_LAN beschriebene **Informationsflusskontrolle**, erzwingt der EVG, dass *zu schützende Daten der TI und der Bestandsnetze* und *zu schützende Nutzerdaten* über den VPN-Tunnel in die Telematikinfrastruktur bzw. zum Internet versendet werden; EVG verhindert ungeschützten Zugriff auf das Transportnetz. Darüber hinaus wurden keine weiteren Regeln ergänzt.

FMT_MSA.3/NK.PF Static attribute initialisation

Restriktive Paketfilter-Regeln

Dependencies: FMT_MSA.1 Management of security attributes

hier erfüllt durch: FMT_MSA.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1/NK

FMT_MSA.3.1/NK.PF The TSF shall enforce the *PF SFP*[44] to provide restrictive[45] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [*administrators* (*local administrator, super administrator)*] to specify alternative initial values to override the default values when an object or information is created.

Refinement: Bei den Sicherheitsattributen handelt es sich um die Filterregeln für den dynamischen Paketfilter (FDP_IFF.1.2/NK.PF). *Restriktive* bedeutet, dass Verbindungen, die nicht ausdrücklich erlaubt sind, automatisch verboten sind. Außerdem muss der EVG bei Auslieferung mit einem Regelsatz ausgeliefert werden, der bereits einen grundlegenden Schutz bietet.

[44] [assignment: *access control SFP, information flow control SFP*]

[45] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

Anwendungshinweis 69: Der Netzkonnektor unterscheidet intern zwischen den Rollen local administrator und super administrator. Alle administrativen Rollen können alternative Default-Werte im Sinne von FMT_MSA.3/PF spezifizieren.

Erläuterung: FMT_MSA.3/NK.PF erfüllt die Abhängigkeit von FDP_IFF.1/NK.PF, weil es die Festlegung von Voreinstellungen für die Paketfilter-Regeln fordert und klärt, welche Rollen die Voreinstellungen ändern können.

Die hier noch nicht erfüllten Abhängigkeiten (FMT_MSA.1/NK.PF und FMT_SMR.1/NK) werden in Abschnitt 6.2.6 Administration diskutiert.

6.2.3. Netzdienste

Zeitsynchronisation

FPT_STM.1/NK Reliable time stamps

Der EVG stellt verlässliche Zeitstempel bereit, indem er die Echtzeituhr gemäß OE.NK.Echtzeituhr regelmäßig synchronisiert.

Dependencies: No dependencies.

FPT_STM.1.1/NK The TSF shall be able to provide reliable time stamps.

Refinement: Die Zuverlässigkeit (*reliable*) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [22] erreicht.

Der EVG verwendet den verlässlichen Zeitstempel für sich selbst und bietet anderen Konnektorteilen eine Schnittstelle zur Nutzung des verlässlichen Zeitstempels an.

Befindet sich der EVG im Online-Modus, muss er die Zeitsynchronisation mindestens bei Start-up, einmal innerhalb von 24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht [*nicht mehr als 330ms*] von der Zeitinformation der darüber liegenden Stratum Ebene ab.

Anwendungshinweis 70: Zum Zeitdienst siehe Konnektor-Spezifikation [16], Abschnitt 4.2.5 Zeitdienst.

Anwendungshinweis 71: Die im Refinement angegebene Zeitsynchronisation entspricht den Anforderungen der Konnektor-Spezifikation [16] (einmal innerhalb von 24 Stunden).

Anwendungshinweis 72: Gemäß Konnektor-Spezifikation [16], Abschnitt 3.3 Betriebszustand, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [16]

- *Im Betrieb MUSS der Zustand des Konnektors erkennbar sein. Zur Anzeige des Betriebszustandes des Konnektors SOLL es eine Signaleinrichtung am Konnektor geben***.** [TIP1-A_4843].

Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, die den Betriebszustand (Power, Verbindungsstatus, Fehlerzustand) am Konnektorgehäuse anzeigen, um die benannte Anforderung der Spezifikation umzusetzen, siehe LS9 und PS5 in Kapitel 1.3.3

Der NK (EVG in diesem Security Target) meldet bei einer nicht erfolgten Zeitsynchronisation dem AK den Fehlerzustand, so dass dieser via Ereignisdienst seine Benutzer informieren kann. Zusätzlich wird an der Signaleinrichtung der kritische Betriebszustand angezeigt.

Zertifikatsprüfung

FPT_TDC.1/NK.Zert Inter-TSF basic TSF data consistency

Prüfung der Gültigkeit von Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.Zert The TSF shall provide the capability to consistently interpret *information – distributed in the form of a TSL (Trust-Service Status List) and CRL (Certificate Revocation List) information – about the validity of certificates and about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects*[46] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[47] when interpreting the TSF data from another trusted IT product.

Refinement: Der EVG muss prüfen, dass (i) das Zertifikat des Ausstellers (der CA) des VPN-Konzentrator-Zertifikats in der TSL enthalten ist, dass (ii) das Gerätezertifikat nicht in der zugehörigen CRL enthalten ist, dass (iii) sowohl TSL als auch CRL integer sind, d.h., nicht verändert wurden (durch Prüfung der Signatur dieser Listen) und dass (iv) sowohl TSL als auch CRL aktuell sind.

Anwendungshinweis 73: Die interpretation rules in FPT_TDC.1.2/NK.Zert entsprechen der Konnektor-Spezifikation [16]. Der Konnektor prüft insbesondere auch die Integrität der TSL; die Modellierung mit SFRs aus der Familie FCS_COP erfolgt jedoch gemäß [12] im Teil Anwendungskonnektor (XML-Signaturprüfung).
Darüber hinaus muss der Konnektor die für den Download der Hash-Datei der TSL(ECC-RSA) genutzte Verbindung zum TSL-Dienst durch TLS absichern und die Anforderungen aus A_17661 [16] umsetzen.

Anwendungshinweis 74: Die TSL und die CRL muss gemäß Anforderung A_4684 in der Konnektor-Spezifikation [16] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden.

---

46 [assignment: *list of TSF data types*]

47 [assignment: *list of interpretation rules to be applied by the TSF*] (die Regeln werden teilweise im Refinement angeführt)

Der Konnektor kann die TSL und die CRL bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [16]).

Im Rahmen der ECC-Migration muss der Konnektor bei der Initialisierung des neuen Vertrauensankers (ECC-RSA) Cross-Zertifikate verwenden (vgl. A_17837-01 und A_17821) und das TSL-Signer-CA-Zertifikat (ECDSA) als TI-Vertrauensanker und die TSL(ECC-RSA) verwenden (A_17688). Zur Signaturprüfung der TSL werden die Vorgaben aus A_17205 und A_21185 berücksichtigt. Der EVG speichert den neuen TI-Vertrauensanker im sicheren Datenspeicher (gem. A_17548 [16]). Im Rahmen der Aktualisierung der TSL werden die Vorgaben aus TIP1-A_4693-02 in [16] umgesetzt. Dabei wird sichergestellt, dass, abweichend von anderen Fällen, in denen lediglich die eingebettete XML-Signatur geprüft werden, bei einem TSL Download aus dem Internet die detached signature vom Konnektor heruntergeladen und geprüfen wird.

6.2.4. Stateful Packet Inspection

Weitergehende Angriffe gegen die Systemintegrität des EVG werden abgewehrt (robuste Implementierung, Resistenz gegen Angriffe wie von AVA_VAN.5 gefordert), aber nicht im Detail erkannt, , d.h. eine komplexe Erkennungslogik ist weder gefordert noch implementiert.Der Aspekt der Stateful Packet Inspection wird durch FDP_IFF.1.4/NK.PF modelliert.

6.2.5. Selbstschutz

Speicheraufbereitung

FDP_RIP.1/NK Subset residual information protection

Speicheraufbereitung (Löschen nicht mehr benötigter Schlüssel direkt nach ihrer Verwendung durch aktives Überschreiben); keine dauerhafte Speicherung medizinischer Daten.

Dependencies: No dependencies.

FDP_RIP.1.1/NK The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[48] the following objects: *cryptographic keys (and session keys) used for the VPN or for TLS-connections, user data (zu schützende Daten der TI und der Bestandsnetze and zu schützende Nutzerdaten),* [*none*][49].

Refinement: Die sensitiven Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. Reset überschrieben werden.

Anwendungshinweis 75: Der Konnektor speichert zu schützende Daten der TI und der Bestandsnetze oder zu schützende Nutzerdaten niemals dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z. B. während einer Ver- oder Entschlüsselung).

---

48 [selection: *allocation of the resource to*, *deallocation of the resource from*]

49 [assignment: *list of objects*]

Selbsttests

FPT_TST.1/NK TSF testing

Selbsttests

Dependencies: No dependencies.

FPT_TST.1.1/NK The TSF shall run a suite of self tests [during initial start-up][50] to demonstrate the correct operation of [the TSF][51].

FPT_TST.1.2/NK The TSF shall provide authorised users with the capability to verify the integrity of TSF data[52].

FPT_TST.1.3/NK The TSF shall provide authorised users with the capability to verify the integrity of [TSF][53] .

Refinement: Zur Erfüllung der Anforderungen aus FPT_TST.1/NK muss der EVG mindestens die Mechanismen implementieren, welche dem aktuellen Stand der Technik bei Einzelplatz-Signaturanwendungen entsprechen. Dazu gehören insbesondere:

- die Prüfung kryptographischer Verfahren bei Programmstart,
- eine Prüfung der korrekten Funktionalität und Qualität des RNG, sofern der EVG einen physikalischen Zufallszahlen-generator beinhaltet und diesen anstelle des Umgebungsziels OE.NK.RNG nutzt.

Anwendungshinweis 76: Die kryptographischen Verfahren werden in Software implementiert. Der Benutzer kann die self tests durch Neustart des EVGs selbst anstoßen. Die im Refinement geforderten Mechanismen werden wie folgt umgesetzt:

- Eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (z. B. Konfigurationsdateien, TSF-Daten) mit kryptographischen Verfahren beim Programmstart

Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K (OE.NK.RNG) als Seed Quelle für den Zufallszahlengenerator des Betriebssystems. Es werden keine weiteren physikalischen Zufallszahlengeneratoren verwendet.

Schutz von Geheimnissen, Seitenkanalresistenz

Zur Definition der Anforderung FPT_EMS.1/NK siehe Abschnitt 5.1.

FPT_EMS.1/NK Emanation of TSF and User data

Dependencies: No dependencies.

---

50 [selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorised user*, *at the conditions* [assignment: *conditions under which self test should occur*]]

51 [selection: [assignment: *parts of TSF*], *the TSF*]

52 [selection: [assignment: *parts of TSF data*], *TSF data*]

53 [selection: [assignment: *parts of TSF*], *TSF*]

FPT_EMS.1.1/NK The TOE shall not emit *sensitive data (as listed below) – or information which can be used to recover such sensitive data – through network interfaces (LAN or WAN)*[54] in excess of *limits that ensure that no leakage of this sensitive data occurs*[55] enabling access to

- *session keys derived in course of the Diffie-Hellman-Keyexchange-Protocol,*
- *[none]*[56],
- *[none]*[57],
- *[none]*[58],
- *[key material used for authentication of administrative users]*[59],
- *[passwords used for authentication of administrative users]*[60] and
- *data to be protected ("*zu schützende Daten der TI und der Bestandsnetze")
- *[none]*[61].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)*[62] are unable to use the following interface *WAN interface or LAN interface of the connector*[63] to gain access to **the sensitive data (TSF data and user data) listed above**[64].

Anwendungshinweis 77: Es wurden keine weiteren Verfeinerungen vorgenommen. Die Integritätsprüfung bei Selbsttest und Software-Update erfolgt anhand von öffentlichen Signatur-Schlüsseln. Die Software Images werden über einen sicheren Kanal (VPN/TLS) übertragen. Die Images selbst sind dabei unverschlüsselt. Für die entsprechenden Auswahl Operationen des PPs [11] wurde daher „none" gewählt. Die Authentisierung des Administrators wird vom Netzkonnektor durchgeführt. Dieser schützt die Authentisierungsschlüssel und Passwörter vor Offenlegung.

---

54 [assignment: *types of emissions*]

55 [assignment: *specified limits*]

56 *[selection: none, key material used to verify the TOE's integrity during self tests]*

57 *[selection: none, key material used to verify the integrity and authenticity of software updates]*

58 *[selection: none, key material used to decrypt encrypted software updates (if applicable)]*

59 *[selection: none, key material used for authentication of administrative users (if applicable)]*

60 [assignment: *list of types of TSF data*]
Hinweis: Die Auswahlen (*selection*) wurde vom PP-Autor im Rahmen des *assignments* hinzugefügt; diese Auswahlen sind optional.

61 [assignment: *list of types of user data*]

62 [assignment: *type of users*]

63 [assignment: *type of connection*]

64 refinement (Umformulierung) sowie Zuweisung der beiden *assignments*: [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*]

Sicherheits-Log

FAU_GEN.1/NK.SecLog Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

hier erfüllt durch: FPT_STM.1/NK

FAU_GEN.1.1/NK.SecLog The TSF shall be able to generate an audit record of the following auditable events:

b) All auditable events for the [not specified][65] level of audit; and

c)

- *start-up, shut down and reset (if applicable) of the TOE*
- *VPN connection to TI successfully / not successfully established,*
- *VPN connection to SIS successfully / not successfully established,*
- *TOE cannot reach services of the transport network,*
- *IP addresses of the TOE are undefined or wrong,*
- *TOE could not perform system time synchronisation within the last 30 days,*
- *during a time synchronisation, the deviation between the local system time and the time received from the time server exceeds the allowed maximum deviation (see refinement to FPT_STM.1/*NK*);*
- *changes of the TOE configuration.*[66]

operational states according to [16], table 3[67]

Refinement: Der in CC angegebene *auditable event a) Start-up and shutdown of the audit functions* ist nicht relevant, da die Generierung von Sicherheits-Log-Daten nicht ein- oder ausgeschaltet werden kann.

FAU_GEN.1.2/NK.SecLog The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*][68].

---

65 [selection, choose one of: *minimum, basic, detailed, not specified*]

66 [assignment: *other specifically defined auditable events*]

67 refinement

68 [assignment: *other audit relevant information*]

Refinement: Das Sicherheits-Log muss in einem nicht-flüchtigen Speicher abgelegt werden, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher muss hinreichend groß dimensioniert sein. Der Speicher ist dann hinreichend groß dimensioniert, wenn sichergestellt ist, dass ein Angreifer durch das Provozieren von Einträgen im Sicherheits-Log die im Rahmen einer Log-Auswertung noch interessanten Log-Daten nicht unbemerkt aus dem Speicher verdrängen kann.

Anwendungshinweis 78: Es werden alle in der Konnektor-Spezifikation [16] (Abschnitte 3.2 und 3.3, Tabelle 3) aufgeführten Fehlerzustände protokolliert. Die Konnektor-Spezifikation fordert die Initialisierung des Protokollierungsdienstes und weiterer Dienste in der Boot-Phase und die Meldung des Abschlusses der Boot-Phase durch den Event "BOOTUP/ BOOTUP_COMPLETE". Der Protokollierungsdienst wird als erster Dienst gestartet; dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „start up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet. Analog wird der Protokollierungsdienst als letzter Dienst bei einem shut-down des EVG beendet und ensprechend als Zeitpunkt für das Ereignis „shut down“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet.

Anwendungshinweis 79: Der Netzkonnektor muss auf einer HW betrieben werden, die ausreichend Speicherplatz für die Log-Einträge zur Verfügung stellt, siehe Kapitel 1.3.6. Zusätzlich implementiert der Netzkonnktor die folgenden Mechanismen um die sichere Protokollierung von Ereignissen zu gewährleisten: Zusammenfassung aufeinanderfolgender Einträge gleicher Ereignisse mit Angabe der Anzahl, Log Rotation und Komprimierung archivierter Logs.

FAU_GEN.2/NK.SecLog User identity association

Dependencies: FAU_GEN.1 Audit data generation

hier erfüllt durch: FAU_GEN.1/NK.SecLog

FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

FAU_GEN.2.1/NK.SecLog For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Anwendungshinweis 80: Der EVG nimmt bei Konfigurationsänderungen durch authentisierte Administratoren (username, password) die Identität des ändernden Administrators (username) und die die jeweilige Administrator-Rolle in das Sicherheits-Log auf.

6.2.6. Administration

Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung

FMT_SMR.1/NK Security roles

Dependencies: FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

FMT_SMR.1.1/NK The TSF shall maintain the roles

- *Administrator* ***(local administrator, super administrator)***[69],
- *SIS,*
- *TI*
- *Anwendungskonnektor*[70].

FMT_SMR.1.2/NK The TSF shall be able to associate users with roles.

Refinement: Die TSF erkennen die in FMT_SMR.1.1 definierte Rolle Administrator daran, dass das Sicherheitsattribut „Autorisierungsstatus“ des Benutzers „Administrator“ den Wert „autorisiert“ besitzt (wie von FMT_MSA.4/NK gesetzt).

Anwendungshinweis 81: Der EVG unterstützt die Rolle Administrator.

Anwendungshinweis 82: In einem Gesamtkonnektor kann der Administrator des Netzkonnektors auch als NK-Administrator bezeichnet werden. – Externe vertrauenswürdige IT-Systeme wie Kartenterminals sind keine Rollen, also ohne Einfluss auf FMT_SMR.1/NK. Lediglich der Anwendungskonnektor wurde hier formal als Rolle definiert, da er das Sicherheitsverhalten von Funktionen des EVG steuern kann, siehe FMT_MOF.1/NK.TLS. Die Rollen SIS und TI werden nur im Zusammenhang mit den Paketfilterregeln für die Kommunikation mit deren VPN-Konzentratoren verwendet.

FMT_MTD.1/NK Management of TSF data

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1/NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

FMT_MTD.1.1/NK The TSF shall restrict the ability to [query, modify, delete, clear, [*activate/deactivate (VPN connection)*]][71] the *real time clock, packet filtering rules [VPN connection]*[72] to *the role Administrator*[73]. **The TSF shall restrict the ability to modify the configuration for automatic installation of software updates.**

Refinement: Die *real time clock* bezieht sich auf die von OE.NK.Echtzeituhr geforderte Echtzeituhr. Obwohl die Echtzeituhr in der Umgebung liegt, wird ihre Zeit vom EVG genutzt und der EVG beschränkt den Zugriff (*modify* = Einstellen der Uhrzeit) auf diese Echtzeituhr. Die

69 refinement

70 [assignment: *the authorised identified roles*]

71 [selection: *change_default*, *query*, *modify*, *delete*, *clear*, [assignment: *other operations*]]

72 [assignment: *list of TSF data*]

73 [assignment: *the authorised identified roles*]

packet filtering rules legen das Verhalten des Paketfilters (O.NK.PF_LAN, O.NK.PF_WAN) fest.

Anwendungshinweis 83: Nur Administratoren dürfen administrieren: Die aufgelisteten administrativen Tätigkeiten können nur von Administratoren ausgeführt werden. Die Operationen *query* und *modify* sind auf die *real time clock* anwendbar. Die Operationen *query, modify, delete* und *clear* können auf die *packet filtering rules* angewended werden. Für die *VPN connection* sind nur die Operationen *activate* und *deactivate* zulässig.

Anwendungshinweis 84: Nur der Administrator kann das Deaktivieren der VPN-Verbindung vornehmen. Die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ wurde in die Liste bei FMT_SMF.1/NK aufgenommen. Innerhalb von FMT_MTD.1/NK wird der Zugriff auf diese Managementfunktion auf den Administrator beschränken.

FIA_UID.1/NK.SMR Timing of identification

Identification of Security Management Roles

Dependencies: No dependencies.

FIA_UID.1.1/NK.SMR The TSF shall allow *the following TSF-mediated actions:*

- *all actions except for administrative actions (as specified by FMT_SMF.1/*NK*, see below)*[74]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/NK.SMR The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Anwendungshinweis 85: Die Zuweisung all actions except for administrative actions (as specified by FMT_SMF.1/NK) wird in diesem Security Target nicht weiter eingeschränkt. Vor administrativen Tätigkeiten ist die Identifikation verpflichtend.

FTP_TRP.1/NK.Admin Trusted path

Trusted Path für den Administrator.

Dependencies: No dependencies.

FTP_TRP.1.1/NK.Admin The TSF shall provide a communication path between itself and [*local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure][75]

FTP_TRP.1.2/NK.Admin The TSF shall permit [the TSF, local users][76] to initiate communication via the trusted path.

---

74 [assignment: *list of TSF-mediated actions*]

75 [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]

76 [selection: *the TSF, local users, remote users*]

FTP_TRP.1.3/NK.Admin The TSF shall require the use of the trusted path for *initial user authentication and administrative actions*.[77]

Anwendungshinweis 86: Die Wartung kann über nur die LAN-Schnittstelle (PS2) erfolgen.

FMT_SMF.1/NK Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1/NK The TSF shall be capable of performing the following security management functions:

- *Management of dynamic packet filtering rules (as required for FDP_IFC.1/NK.*PF*, FDP_IFF.1/NK.*PF*, FMT_MSA.3/NK.*PF*, and FMT_MSA.1/NK.*PF*).*

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

- *Management of TLS-Connections (as required for FMT_MOF.1/NK.TLS).*

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.) [78]

- **Aktivieren und Deaktivieren des VPN-Tunnels**[79]

Anwendungshinweis 87: Das Review (Lesen und Auswerten) der von FAU_GEN.1/NK.SecLog erzeugten Audit-Daten wird nicht als Managementfunktion modelliert.

FMT_MSA.1/NK.PF Management of security attributes

Nur der Administrator darf (gewisse) Filterregeln verändern.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1/NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

FMT_MSA.1.1/NK.PF The TSF shall enforce the *PF SFP*[80] to restrict the ability to *[query, modify, delete]*[81] the security attributes *packet filtering*

---

77 [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

78 [assignment: *list of management functions to be provided by the TSF*]

79 refinement: **Aktivieren und Deaktivieren des VPN-Tunnels**

80 [assignment: *access control SFP*, *information flow control SFP*]

81 *[selection: query, modify, delete, [assignment: other operations]]*

rules[82] to *the roles „Administrator“, [no other authorised identified roles]*[83].

Refinement: Der Administrator darf nur solche Filterregeln (*packet filtering rules*) administrieren, welche die Kommunikation zwischen dem Konnektor und Systemen im LAN betreffen. Firewall-Regeln, welche

- die Kommunikation zwischen dem Konnektor einerseits und dem Transportnetz, der Telematikinfrastruktur, sowohl gesicherte als auch offene Fachdienste und zentrale Dienste, bzw. den Bestandsnetzen andererseits oder
- die Kommunikation zwischen dem LAN einerseits und dem Transportnetz, der Telematikinfrastruktur sowohl gesicherte als auch offene Fachdienste und zentrale Dienste, bzw. den Bestandsnetzen (außer Freischalten aktiver Bestandsnetze) andererseits

betreffen, dürfen nicht über die Administrator-Schnittstelle verändert werden können. Der Administrator muss den gesamten WAN-seitigen Verkehr blockieren können (siehe Konnektorspezifikation [16], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [16], Kapitel 4.2.1.2, ANLW_FW_SIS_ADMIN_RULES) festlegen. Vorgabewerte dürfen nicht verändert werden („change-default“ ist nicht erlaubt).

Erläuterung: FMT_MSA.1/NK.PF sorgt als von FMT_MSA.3/NK.PF abhängige Komponente dafür, dass die Regeln für den Paketfilter (*packet filtering rules*, diese Regeln werden als security attributes angesehen) nur durch den Administrator oder eine andere kompetente Instanz (siehe FMT_SMR.1/NK) verändert werden können. Weiterhin legt die Konnektorspezifikation [16] fest, dynamisches Routing zu deaktivieren. Dies ist Gegenstand der Schwachstelleanalyse.

Das Refinement minimiert das Risiko, dass durch menschliches Versagen oder Fehlkonfiguration versehentlich ein unsicherer Satz von Filterregeln aktiviert wird. Es sorgt dafür, dass grundlegende Regeln, welche die Kommunikation zwischen dem Konnektor und dem Transportnetz bzw. der Telematikinfrastruktur oder auch die Kommunikation zwischen dem LAN und dem Transportnetz bzw. der Telematikinfrastruktur betreffen, nicht durch einen administrativen Eingriff (Konfiguration) des Administrators außer Kraft gesetzt werden können.

---

[82] [assignment: *list of security attributes*]

[83] [assignment: *the authorised identified roles*]

Anwendungshinweis 88: Unter „*Administrator"* werden hier alle Administrator-Rollen verstanden (local, super). Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [16] definierten Anforderungen.

Anwendungshinweis 89: Firewall-Regeln, die nicht durch den Administrator angepasst werden dürfen, können durch das Einspielen eines Software-Updates aktualisiert werden.

Anwendungshinweis 90: Der Netzkonnektor kann seine Filterregeln abhängig von Ereignissen anderer Konnektorteile (z. B. Anwendungskonnektor) dynamisch anpassen.

FMT_MSA.4/NK Security attribute value inheritance

Definition von Regeln für die Sicherheitsattribute

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_MSA.4.1/NK The TSF shall use the following rules to set the value of security attributes:

Die Authentisierung des Administrators ***~~kann gemäß OE.NK.Admin_Auth in der IT-Einsatzumgebung erfolgen~~ wird durch den Netzkonnektor selbst durchgeführt***[84]

Wenn die Authentisierung des Administrators ***~~in der IT-Einsatzumgebung erfolgt und~~***[85] *erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diese Autorisierung und weisen dem Sicherheitsattribut „Autorisierungsstatus" des auf diese Weise authentisierten Benutzers „Administrator" den Wert „****autorisiert****" zu.*

Wenn die Authentisierung des Administrators ***~~in der IT-Einsatzumgebung erfolgt und~~***[86] *nicht erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diesen Status und weisen dem Sicherheitsattribut „Autorisierungsstatus" des auf diese Weise nicht authentisierten Benutzers „Administrator" den Wert „****nicht autorisiert****" zu.*[87]

Subjekt	Sicherheitsattribut	Mögliche Werte
Administrator	Autorisierungsstatus	autorisiert, nicht autorisiert

[84] refinement

[87] [assignment: *rules for setting the values of security attributes*] (die Schriftauszeichnungen im Zuweisungstext dienen (wenn nicht explizit durch Fussnoten gekennzeichnet) der besseren Leserlichkeit und kennzeichnen hier keine ausgeführten Operationen)

Hinweis: Die Authentisierung des Administrators erfolgt gemäß O.NK.Admin_Auth durch den Netzkonnektor selbst. OE.NK.Admin_Auth wird daher als automatisch erfüllt betrachtet.

Software Update

FDP_ACC.1/NK.Update Subset access control / Update

Zugriffskontrolle – Updates

Dependencies: FDP_ACF.1 Security attribute based access control

Hier erfüllt durch: FDP_ACF.1/NK.Update.

FDP_ACC.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][88] on

[*subjects:*

(1) Administrator (S_Administrator),

(2) Anwendungskonnektor (S_AK),

(3) Netzkonnektor (S_NK);

objects:

(1) Update-Pakete

operations:

(1) Importieren

(2) Verwenden][89]

Operation	Beschreibung	Anmerkung
Importieren	Einlesen von bereitgestellten Update-Paketen und Aktualisieren der Komponenten des EVG.	Der Download kann automatisch erfolgen.
Verwenden	Die Update-Pakete werden zum Update der TSF-Daten, zum Update des EVG zu einem neuen EVG oder zum Update anderer externer Komponenten (eHealth-Kartenterminal) verwendet.	Das Installieren (Verwenden) des Updates kann automatisch erfolgen.

[88] [assignment: *access control SFP*]

[89] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Hinweis: Das vorgenannte SFR wurde wortgenau aus dem BSI-CC-PP-0098-V3-2021-MA-03 übernommen und enthält daher die Unterscheidung der Subjekte S_Administrator, S_AK und S_NK.

FDP_ACF.1/NK.Update Security attribute based access control / Update

Sicherheitsattribute für Zugriffskontrolle – Updates.

Dependencies: FDP_ACC.1 Subset access control

hier erfüllt durch: FDP_ACC.1/NK.Update

FMT_MSA.3 Static attribute initialisation

nicht erfüllt mit folgender Begründung: Für das Datenobjekt Update-Paket findet keine Initialisierung von Sicherheitsattributen im Sinne von FMT_MSA.3 statt. Signatur und Software Version können nicht sinnvoll vom EVG mit Default Werten initialisiert werden.

FDP_ACF.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][90] to objects based on the following:

[*subjects:*

(1) S_Administrator,

(2) S_AK,

(3) S_NK,

objects:

(1) Update-Pakete with security attributes:

a) Signatur,

b) Zulässige Software-Versionen

][91]

FDP_ACF.1.2/NK.Update The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

(1) Das Subjekt S_AK oder S_NK darf nur Update-Pakete importieren, deren Signatur erfolgreich geprüft wurde.

(2) Die Subjekte S_Administrator, S_AK und S_NK dürfen nur Update-Pakete verwenden, die einer Firmwaregruppe

[90] [assignment: *access control SFP*]

[91] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist.

]92

FDP_ACF.1.3/NK.Update The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*]93.

FDP_ACF.1.4/NK.Update The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

[

(1) S_AK und S_NK dürfen Update-Pakete nicht automatisch anwenden, wenn das automatische Anwenden von Update-Paketen nicht durch S_Administrator aktiviert wurde.

(2) Wenn MGM_LU_ONLINE=Disabled gesetzt ist, so darf die TSF keine Kommunikation mit dem Update-Server (KSR) herstellen.

]94

Hinweis: Das vorgenannte SFR wurde wortgenau aus dem BSI-CC-PP-0098-V3-2021-MA-03 übernommen und enthält daher die Unterscheidung der Subjekte S_Administrator, S_AK und S_NK.

Anmerkung: Die Integrität und Authentizität der Update-Dateien wird durch die Verifikation von kryptografischen Signaturen geprüft. Dabei werden Signaturen nach RSASSA-PKCS1-v1_5 with SHA256 (siehe [24]) und 2048 Bit Schlüssellänge verwendet. Die XML-Dateien UpdateInfo.xml und FirmwareGroupInfo.xml werden durch Signaturen nach RSASSA-PSS with SHA256 (siehe [24]) und 2048 Bit Schlüssellänge geschützt.

FTP_ITC.1/NK.KSR Inter-TSF trusted channel / Zum KSR (Update-Server)

Import von Update-Paketen.

Dependencies: No dependencies

Hierarchical to: No other components

FTP_ITC.1.1/NK.KSR The TSF shall provide a communication channel between itself and **S_KSR** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_KSR mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and** ~~or~~ disclosure.

---

92 [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

93 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

94 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FTP_ITC.1.2/NK.KSR The TSF shall permit the TSF[95] to initiate communication via the trusted channel

FTP_ITC.1.3/NK.KSR The TSF shall initiate communication via the trusted channel for Prüfung auf neue Firmware-Update-Pakete und Download neuer Firmware-Update-Pakete[96].

FDP_UIT.1/NK.Update Data exchange integrity / Update

Integrität von Update-Paketen.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_ACC.1/NK.Update

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

hier erfüllt durch: FTP_ITC.1/NK.KSR

FDP_UIT.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][97] to [receive][98] user data ~~**in a manner**~~[99] protected from [modification, deletion, insertion][100]

FDP_UIT.1.2/NK.Update The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion][101] has occurred.

[95] [selection: the TSF, another trusted IT product]

[96] [assignment: list of functions for which a trusted channel is required]

[97] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[98] [selection: *transmit, receive*]

[99] refinement

[100] [selection: *modification, deletion, insertion, replay*]

[101] [selection: *modification, deletion, insertion, replay*]

6.2.7. Kryptographische Basisdienste

Anwendungshinweis 91: Die SFR der Familie FCS in CC Teil 2 [2] enthalten ein [assignment: cryptographic algorithm]. Diese Zuweisungen wurden durch das PP [11] in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI vorgenommen. Die TSF implementieren die darüberhinausgehenden verpflichtenden Vorgaben der angegebenen Standards soweit sie die angegebenen Algorithmen und Protokollen betreffen; es wird dabei den angegebenen Standards mit Ausnahme der zugewiesenen Kryptoalgorithmen nicht widersprechen. So fordert RFC 3602 die Unterstützung von AES 128 Bit, die Zuweisung des SFR FCS_COP.1/NK.ESP aber in Übereinstimmung mit der Spezifikation kryptographischer Algorithmen in der Telematikinfrastruktur [18] an seiner Stelle verbindlich den stärkeren AES 256 Bit. Die Zuweisung erfordert nicht, dass die TSF alle in den angegeben Standards zulässigen Optionen für die spezifizierten kryptographischen Operationen und Schlüsselmanagement-funktionen implementieren muss. Die Anforderungen an die Gewährleistung der Interoperabilität sind hiervon nicht betroffen.

Anwendungshinweis 92: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Die AES Implementierung des TOEs verwendet keine zusätztlichen HW Mechanismen (AES-NI) zur Berechnung der AES-Verschlüsselungen und –Entschlüsselung.

FCS_COP.1/NK.Hash Cryptographic operation

Zu unterstützende Hash-Algorithmen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Alle bisher für FCS_COP.1/NK.Hash genannten Abhängigkeiten werden nicht erfüllt. Begründung: Bei einem Hash-Algorithmus handelt es sich um einen kryptographischen Algorithmus, der keine kryptographischen Schlüssel verwendet. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels und zu seiner Zerstörung erforderlich.

FCS_COP.1.1/NK.Hash The TSF shall perform *hash value calculation*[102] in accordance with a specified cryptographic algorithm *SHA-1, SHA-256, [none]*[103] and cryptographic key sizes *none*[104] that meet the following: *FIPS PUB 180-4 [25].*[105]

[102] [assignment: *list of cryptographic operations*]

[103] *[assignment: list of SHA-2 Algorithms with more than 256 bit size]*

[104] [assignment: *cryptographic key sizes*]

[105] [assignment: *list of standards*]

Refinement: Der Hash-Algorithmus SHA-1 ist im Kontext IPsec ausschließlich für das hash&URL-Verfahren zulässig.

FCS_COP.1/NK.HMAC Cryptographic operation

Zu unterstützende Hash basierende MAC-Algorithmen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.HMAC The TSF shall perform *HMAC value generation and verification*[106] in accordance with a specified cryptographic algorithm *HMAC with SHA-256*, [none][107] and cryptographic key sizes [*128 bit and 256 bit*][108] that meet the following: *FIPS PUB 180-4 [25], RFC 2404 [34], RFC 4868 [35], RFC 7296 [31].*[109]

FCS_COP.1/NK.Auth Cryptographic operation

Authentisierungs-Algorithmen, die im Rahmen von Authentisierungsprotokollen zum Einsatz kommen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

Die hier genannten Abhängigkeiten werden nicht erfüllt. Begründung: Die *signature creation* wird von der gSMC-K durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* kann auch im EVG durchgeführt werden. Die entsprechenden öffentlichen Schlüsselobjekte werden durch den Import von Zertifikaten in den EVG eingebracht, die Abhängigkeit wird inhaltlich durch FPT_TDC.1/NK.Zert erfüllt.

FCS_CKM.4 Cryptographic key destruction

[106] [assignment: *list of cryptographic operations*]

[107] *[assignment: list of SHA-2 Algorithms with more than 256bit size]*

[108] [assignment: *cryptographic key sizes*]

[109] [assignment: *list of standards*]

hier erfüllt durch: FCS_CKM.4/NK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.

FCS_COP.1.1/NK.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K storing the signing key ID.AK.AUT and performing the RSA operation* [110]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[111] and cryptographic key sizes *2048 bit*[112] and ECDSA OID 1.2.840.10045.4.3.2 or 1.2.840.10045.4.3.3 that meet the following: *RFC 8017 (RSASSA-PKCS1-v1_5) [24], FIPS PUB 180-4 [25]*[113].

FCS_COP.1/NK.ESP Cryptographic operation

Zu unterstützende Verschlüsselungs-Algorithmen für die IPsec-Tunnel in FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.ESP The TSF shall perform *symmetric encryption and decryption with Encapsulating Security Payload*[114] in accordance with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42)*[115] and cryptographic key sizes *256 bit*[116] that meet the following: *FIPS 197 [26], RFC 3602 [33], RFC 4303 (ESP) [30],], specification [18]* [117].

FCS_COP.1/NK.IPsec Cryptographic operation

[110] [assignment: *list of cryptographic operations*]

[111] [assignment: *cryptographic algorithm*]

[112] [assignment: *cryptographic key sizes*]

[113] [assignment: *list of standards*]

[114] [assignment: *list of cryptographic operations*]

[115] [assignment: *cryptographic algorithm*]

[116] [assignment: *cryptographic key sizes*]

[117] [assignment: *list of standards*]

Zu unterstützende Verschlüsselungs-Algorithmen für die IPsec-Tunnel in FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.IPsec The TSF shall perform *VPN communication*[118] in accordance with a specified cryptographic algorithm *IPsec-protocol*[119] and cryptographic key sizes *256 bit*[120] that meet the following: *RFC 4301 (IPsec) [27], specification [18]*[121].

FCS_CKM.1/NK Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

hier erfüllt durch: FCS_CKM.2/NK.IKE, FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec und FCS_COP.1/NK.Hash

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRF_HMAC_SHA256*][122] and specified cryptographic key sizes [*128 bit and 256 bit*][123] that meet the following: *RFC 2104 [46], RFC 7296 [31], specification [18], TR-03116 [14]*[124].

[118] [assignment: *list of cryptographic operations*]

[119] [assignment: *cryptographic algorithm*]

[120] [assignment: *cryptographic key sizes*]

[121] [assignment: *list of standards*]

[122] [assignment: *cryptographic key generation algorithm*]

[123] [assignment: *cryptographic key sizes*]

[124] [assignment: *list of standards*]

Anwendungshinweis 93: Für alle mittels FCS_COP.1/... beschriebenen kryptographische Operationen (mit Ausnahme der Hashwertberechnung, siehe FCS_COP.1/NK.Hash) sind kryptographische Schlüssel erforderlich, die entsprechend der Abhängigkeiten von FCS_COP.1 aus CC Teil 2 [2] entweder durch eine Schlüsselgenerierung (FCS_CKM.1) oder durch einen Schlüsselimport (FDP_ITC.1 oder FDP_ITC.2) zu erfüllen sind. In diesem Security Target wurde (entsprechend zum PP) eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols seine Sitzungsschlüssel (session keys) für die VPN-Kanäle ableitet; diese Ableitung wird als Schlüsselgenerierung angesehen. (Der Aspekt des Schlüsselaustausches mit einem VPN-Konzentrator wird als FCS_CKM.2/NK.IKE modelliert, siehe unten). Alle erzeugten Schlüssel besitzen mindestens 100 Bit Entropie, damit der EVG resistent gegen Angriffe mit hohem Angriffspotential sein kann.

FCS_CKM.2/NK.IKE Cryptographic key distribution

Schlüsselaustausch symmetrischer Schlüssel im Rahmen des Aufbaus des VPN-Kanals.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.2.1/NK.IKE The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *IPsec IKE v2*[125] that meets the following *standard: RFC 7296 [31], specifications [18], TR-02102-3 [13]*[126].

FCS_CKM.4/NK Cryptographic key destruction

Löschen nicht mehr benötigter Schlüssel.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4.1/NK The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with fixed bit pattern*][127] that meets the following: [*none*][128].

---

[125] [assignment: *cryptographic key distribution method*]

[126] [assignment: *list of standards*]

[127] [assignment: *cryptographic key destruction method*]

[128] [assignment: *list of standards*]

Anwendungshinweis 94: FCS_CKM.4/NK zerstört die von den Komponenten FCS_COP.1/... sowie FCS_CKM.2 (FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE) benötigten Schlüssel. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle verwendeten Schlüssel. Die Schlüssel werden durch das überschreiben mit Nullen oder festen Werten zerstört.

Anwendungshinweis 95: Die Operationen stehen im Einklang mit den in Dokumenten [14], [18] und [16] angegebenen Vorgaben. Dies gilt insbesondere für alle genannten SFRs FCS_COP.1/* sowie FCS_CKM.1/NK, FCS_CKM.2/NK.IKE und FCS_CKM.4/NK. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle definierten Kryptoverfahren.
Der DH-Exponent für den Schlüsselaustausch hat eine Mindestlänge gemäß [18]. Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy wurden die Vorgaben aus [18] beachtet. Sofern der EVG im Rahmen des IKE-Verbindungsaufbaus feststellt, dass der IKE-Responder (VPN-gateway) noch keine ECC-Verfahren unterstützt (INVALID_KE_PAYLOAD-Nachricht), so setzt der EVG die Vorgaben gem. GS-A_4382-* in [18] um (vgl. A_17210).

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Die folgenden SFRs wurden in dieses Security Target aufgenommen, um sicher zu stellen, dass die kryptographischen Sicherheitsanforderungen an die im Konnektor zu nutzenden TLS-Verbindungen nach hoher Angriffsstärke evaluiert werden.

Hinweis 1: Tatsächlich verwendet werden die von der Spezifikation geforderten TLS-Verbindungen erst im Anwendungskonnektor.

Hinweis 2. TLS-Verbindungen werden auch für die Absicherung einer Administrationsschnittstelle des Netzkonnektors verwendet. Die SFRs in diesem Kapitel werden dafür mit genutzt und wurden entsprechend vervollständigt.

FTP_ITC.1/NK.TLS Inter-TSF trusted channel

Grundlegende Sicherheitsleistungen eines TLS-Kanals

Dependencies: No dependencies.

FTP_ITC.1.1/NK.TLS The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and **is able to**[129] provide~~s~~ assured identification of its end points and protection of the channel data from modification **and**[130] disclosure.

[129] refinement: dieses Refinement soll darauf hinweisen, dass der Netzkonnektor die Möglichkeit implementiert, beide Seiten zu authentisieren, dass es aber Entscheidung des nutzenden Systems (i.a. der Anwendungskonnektor) ist, inwieweit diese Authentisierung genutzt wird.

[130] refinement (or → and)

FTP_ITC.1.2/NK.TLS The TSF **must be able to**[131] permit *the TSF or another trusted IT-Product*[132] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.TLS The TSF shall initiate communication via the trusted channel for *communication required by the Anwendungskonnektor, [administration]*[133].

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von unbefugtem Löschen, Einfügen oder Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss auf Basis des TLS-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [16] und [18], wobei TLS 1.2 gemäß RFC 5246 [41] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch und bei der Signaturprüfung mittels ECDSA werden die Kurven P-256 oder P-384 [FIPS-186-5] unterstützt. Daneben werden die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt. Andere Kurven werden nicht verwendet, damit die Ordnung des Basispunktes in E(F_p) nicht zu klein wird. Falls der EVG in der Rolle TLS-Client agiert, so wird er die eben genannten Ciphersuiten gegenüber RSA-basierten Ciphersuiten (vgl. GS-A_4384-01) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5256#7.4.1.2 ClientHello]).

Die Anforderung „assured identification” im ersten Element des SFR impliziert, dass der EVG in der Lage sein muss, die Authentizität des „trusted IT-product“ zu prüfen. Im Rahmen dieser Überprüfung muss er in der Lage sein, eine Zertifikatsprüfung durchführen (siehe FPT_TDC.1/NK.TLS.Zert). Da allerdings der Anwendungskonnektor in Abhängigkeit von der TLS-Verbindung

131 refinement (shall → must be able to)

132 [selection: *the TSF, another trusted IT-Product]*

133 *[assignment: list of other functions for which a trusted channel is required]*

ggf. entscheiden kann, auf eine Authentikation eines der Endpunkte zu verzichten, wurde ein entsprechendes refinement gewählt. Aus demselben Grund wurde dies für die Frage, ob der EVG selbst oder das andere IT-Produkt die Kommunikation anstoßen kann, durch ein refinement präzisiert, da auch dies vom Typ der TLS-Verbindung abhängt und vom Anwendungskonnektor entschieden wird.

Anwendungshinweis 96: Der EVG unterstützt ausschließlich TLS Version 1.2 (s. [18]). Insbesondere unterstützt der EVG alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS; dabei werden die Anforderungen aus [18] erfüllt. Die Kryptosuiten sollen für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt werden. Die TLS Versionen 1.1, 1.0 und SSL werden vom EVG nicht unterstützt. Falls der EVG in der Rolle als TLS-Client agiert, so wird er gem A_17124 die Ciphersuiten TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 gegenüber anderen von ihm unterstützen RSA-basierte Ciphersuiten bevorzugen, d.h. in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5246#7.4.1.2 Client Hello]. Im Rahmen der Erstellung und Prüfung von digitalen Signaturen beim TLS-Handshakes unterstützt der EVG die folgenden Hashfunktion: SHA-256 [FIPS-180-4]. Falls der TLS-Kanal mit älteren eHealth-Kartenterminals nicht mit einem besseren kryptographischen Verfahren aufgebaut werden kann, baut der EVG gem. A_23226-01 den TLS-Kanal unter Verwendung von TLS_DHE_RSA_WITH_AES_128_CBC_SHA oder TLS_DHE_RSA_WITH_AES_256_CBC_SHA auf. Dabei wird für die Schlüsselaushandlung die DH-Gruppe 14 gem. [36] und ein DH-Exponent mit einer Länge von mind. 256 Bit verwendet.

FPT_TDC.1/NK.TLS.Zert Inter-TSF basic TSF data consistency

Prüfung der Gültigkeit von TLS-Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.TLS_Zert The TSF shall provide the capability to consistently interpret

(1) X.509-Zertifikate für TLS-Verbindungen

(2) eine Liste gültiger CA-Zertifikate (Trust-Service Status List TSL)

(3) Sperrinformationen zu Zertifikaten für TLS-Verbindungen, die via OCSP erhalten werden

(4) importierte X.509 Zertifikate für Clientsysteme

(5) eine im Konnektor geführte Whitelist von Zertifikaten für TLS-Verbindungen

(6) [none][134]

when shared between the TSF and another trusted IT product.

[134] *[assignment: additional list of data types]*

FPT_TDC.1.2/NK.TLS_Zert The TSF shall use *interpretation rules*[135] when interpreting the TSF data from another trusted IT product.

Refinement: Die „interpretation rules“ umfassen: Der EVG muss prüfen können, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist oder in einer gültigen Zertifikatskette bis zu einer zulässigen CA (Letzteres ggf. anhand der TSL) enthalten ist. Ebenso muss sie anhand einer OCSP-Anfrage prüfen können, ob das Zertifikat noch gültig ist.

Anwendungshinweis 97: Die interpretation rules entsprechen der Konnektor-Spezifikation [16].

Anwendungshinweis 98: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [16] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden. Der Konnektor kann die TSL bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [16]).

FCS_CKM.1/NK.TLS Cryptographic key generation / TLS

Dependencies: [FCS_CKM.2 Cryptographic key distribution,
or FCS_COP.1 Cryptographic operation]

hier erfüllt durch: FCS_COP.1/NK.TLS.HMAC und FCS_COP.1/NK.TLS.AES

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* [136] and specified cryptographic key sizes *128 bit for AES-128, 256 bit for AES-256, 160 for HMAC with SHA, 256 for HMAC with SHA-256 and 384 for HMAC with SHA-384*[137] that meet the following: *Standard RFC 4346 [40] and RFC 5246 [41].*[138]

[135] [assignment: *list of interpretation rules to be applied by the TSF*] (die Regeln werden teilweise im Refinement angeführt)

[136] [assignment: *cryptographic key generation algorithm*]

[137] [assignment: *cryptographic key sizes*]

[138] [assignment: *list of standards*]

Anwendungshinweis 99: Der unterstützt ausschließlich TLS Version 1.2 (s. [18]). Insbesondere werden vom EVG alle im SFR genannten cipher suites als Algorithmen für TLS unterstützt. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [43]) bzw. dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (ECDHE_RSA nach [44]). Die Auswahloperation zur Schlüssellänge hängt von den gewählten Algorithmen ab. Die Schlüssel werden für die TLS-Kommunikation zwischen dem EVG und anderen Komponenten genutzt. Es werden jeweils getrennte Schlüssel für jede Verwendung und Verschlüsselung nach FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.HMAC berechnet. Der EVG erzeugt Schlüssel mit einer Entropie von mindestens 100 Bit (siehe [14]). Bezüglich Diffie-Hellman-Gruppen für die Schlüsselaushandlung wurden die Vorgaben aus [18] beachtet. Der DH-Exponent für den Schlüsselaustausch hat eine Mindestlänge gemäß [18]. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange werden die gemäß [18] vorgegebenen Kurven unterstützt.
Gem. TIP1-A_4720-03 stellt der EVG sicher, dass nur ECC-basierte Ciphersuits angeboten werden, wenn die Gegenstelle über ECC-Zertifikate verfügt.

FCS_COP.1/NK.TLS.HMAC Cryptographic operation / HMAC for TLS

Zu unterstützende Hash basierende MAC-Algorithmen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
hier erfüllt durch: FCS_CKM.1/NK.TLS
FCS_CKM.4 Cryptographic key destruction
hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.HMAC The TSF shall perform *HMAC value generation and verification*[139] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[140] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[141] that meet the following: *Standards FIPS 180-4 [25] and RFC 2104 [46]*[142].

Anwendungshinweis 100: FCS_COP.1/NK.TLS.HMAC wird für die Integritätssicherung innerhalb des TLS-Kanals benötigt.

[139] [assignment: *list of cryptographic operations*]

[140] [assignment: *cryptographic algorithm*]

[141] [assignment: *cryptographic key sizes*]

[142] [assignment: *list of standards*]

FCS_COP.1/NK.TLS.AES Cryptographic operation

Zu unterstützende Verschlüsselungs-Algorithmen für die TLS Verbindung in FTP_ITC.1/NK.TLS

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.AES The TSF shall perform *symmetric encryption and decryption*[143] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[144] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[145] that meet the following: *FIPS 197 [26],* NIST 800-38D *[42],* RFC 5246*,* RFC 8422 *[44], RFC 5289 [45], specification [18]* [146].

Anwendungshinweis 101: Es gilt Anwendungshinweis 92:.

FCS_COP.1/NK.TLS.Auth Cryptographic operation for TLS

Authentisierungs-Algorithmen, die im Rahmen von TLS zum Einsatz kommen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.Zert und FDP_ITC.2/NK.TLS.

Die *signature creation* wird in der Regel (Ausnahmen s.u.) von der gSMC-K durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* kann auch im EVG durchgeführt werden. Die entsprechenden öffentlichen Schlüsselobjekte werden entweder im EVG erzeugt (FCS_CKM.1/NK.Zert) oder importiert

[143] [assignment: *list of cryptographic operations*]

[144] [assignment: *cryptographic algorithm*]

[145] [assignment: *cryptographic key sizes*]

[146] [assignment: *list of standards*]

(FDP_ITC.2/NK.TLS). Die Interpretation von TLS Zertifikaten wird durch FPT_TDC.1/NK.TLS.Zert erbracht.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.

FCS_COP.1.1/NK.TLS.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K storing the signing key and performing the RSA operation* [147]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[148] and cryptographic key sizes *2048 bit*[149] that meet the following: *RFC 8017 (RSASSA-PKCS1-v1_5) [24], FIPS PUB 180-4 [25]*[150].

Anwendungshinweis 102: Die Signaturberechnung gemäß FCS_COP.1/NK.TLS.Auth wird für die Berechnung digitaler Signaturen zur Authentisierung bei TLS verwendet. Der EVG nutzt dafür bei Verbindungen ins lokale Netz (LAN) des Leistungserbringers die gSMC-K. Der dafür benötigte asymmetrische Schlüssel wurde während der Produktion der gSMC-K importiert oder generiert. Alternativ verwendet der EVG als TLS-Server im Falle von importierten (vgl. FDP_ITC.2/NK.TLS) oder generierten (vgl. FCS_CKM.1/NK.Zert) x509-Zertifikaten zur Signaturerstellung den privaten Schlüssel im Speicher des Konnektors. Für Verbindungen zum WAN wird eine SM-B verwendet die der Anwendungskonnektor ansteuert. Hier wird nur die LAN-seitige TLS-Verbindung modelliert. Die WAN-seitige TLS-Verbindung erfolgt analog und nutzt dieselben kryptografischen Basisdienste für TLS.

Hinweis: Der EVG unterstützt über den in FCS_COP.1/NK.TLS.Auth genannten Algorithmus hinaus gem (A_17124-03) die folgenden Algorithmen:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B)
*TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C)
* als TLS-Client: ecdsa-with-SHA256 auf Basis der Kurve brainpoolP256r1.

ecdsa-with-SHA256 wird vom EVG im Zuge der ECC-Migration (vgl. [18], sec. 5.4) unterstützt. Zu den Hashalgorithmen zur Signaturprüfung vgl. auch Anwendungshinweis 96

FCS_CKM.1/NK.Zert Cryptographic key generation / Certificates

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]

nicht erfüllt mit folgender Begründung: FCS_CKM.1/NK.Zert bietet die Möglichkeit X.509 Zertifikate für die TLS-geschützte

[147] [assignment: *list of cryptographic operations*]

[148] [assignment: *cryptographic algorithm*]

[149] [assignment: *cryptographic key sizes*]

[150] [assignment: *list of standards*]

Kommunikation mit Clientsystemen zu erzeugen. Gemäß FDP_ETC.2/NK.TLS können die Zertifikate und die zugehörigen privaten Schlüssel vom Administrator exportiert werden. Key distribution gemäß FCS_CKM.2 findet nicht statt.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK.Zert The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA Key Pair Generation, Elliptic Curve Key Pair Generation*][151] and specified cryptographic key size 2048 bit[152] and 3072 bit for RSA and 256 bit for ECC with NIST P-256[153] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [23], BSI TR-03116-1 [14]*[154]*, OID 1.2.840.10045.4.3.2, RFC 5639 [23a], BSI-TR-03111 [14a].*[155]

The TSF shall

(1) create a valid X.509 [47] certificate with the generated RSA key pair and

(2) create a PKCS#12 [48] file with the created certificate and the associated private key. [156]

Anwendungshinweis 103: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [18], Anforderung GS-A_4368 umsetzen. Die Verfeinerung zu FCS_CKM.1/NK.Zert soll die Möglichkeit zur Erzeugung von X.509 Zertifikaten für die TLS-geschützte Kommunikation mit Clientsystemen bieten. Ein Export dieser Zertifikate und der zugehörigen privaten Schlüssel (mit Ausnahme des privaten Schlüssel von ID.AK.AUT) ist Gegenstand von FDP_ETC.2/NK.TLS.
Der EVG stellt gem. A_23139 sicher, dass ein öffentlicher ECC-Schlüssel im CA-Zertifikat, die öffentlichen ECC-Schlüssel der zum CA-Zertifikat aus zugehörigen OCSP-Zertifikate (vgl. A_23142), und die öffentlichen ECC-EE-Schlüssel in den EE-Zertifikaten, die durch die CA mit dem Schlüssel prüfbar sind, die gleichen Kurvenparameter (brainpoolP256r1, P-256 etc. gem. [18] Tab_KRYPT_002a besitzen. Zusätzlich zu in FCS_CKM.1.1/NK.Zert genannten Verfahren generiert der EVG auch ECC-Schlüssel mit NIST-Kurven. Brainpool-Kurven werden nicht unterstützt.

FDP_ITC.2/NK.TLS Import of user data with security attributes

[151] [assignment**:** *Algorithm for cryptographic key generation of key pairs*]

[152] [assignment**:** *cryptographic key sizes*]

[153] Refinement: 3072 bit for RSA and 256 bit for ECC with NIST P-256

[154] [assignment**:** *list of standards*]

[155] Refinement: OID 1.2.840.10045.4.3.2, RFC 5639 [36a], BSI-TR-03111 [76b]

[156] refinement

Import von Zertifikaten

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

nicht erfüllt mit folgender Begründung: Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanagt. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen importiert werden. Damit wird diese Abhängigkeit inhaltlich erfüllt.

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

hier erfüllt durch: FTP_TRP.1/NK.Admin

FPT_TDC.1 Inter-TSF basic TSF data consistency

hier erfüllt durch: FPT_TDC.1/NK.TLS.Zert

FDP_ITC.2.1/NK.TLS The TSF shall enforce the *Certificate-Import-SFP*[157] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/NK.TLS The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/NK.TLS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/NK.TLS The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/NK.TLS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) Die TSF importiert X.509 Zertifikate für Clientsysteme durch den Administrator über die Management-Schnittstelle

(2) Die TSF importiert X.509 Zertifikate und Schlüsselmaterial für den EVG gem. A_21697 in [16] durch den Administrator über die Managementschnitstelle

(3) Die TSF importiert die erneuerten Zertifikate des Objekts O_LZV_Zert_gSMCK durch den Administrator über die Managementschnittstelle oder automatisch aus der TI, wenn die existierenden Zertifikate nicht mehr länger als 180 Tage gültig sind

[157] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

(4) Die TSF setzt die Vorgaben aus A_21811- und damit TAB_KON_866 durch durch (keine Unterstützung RSA-2048 und ECC-256 mit brainpool-Kurven; Unterstützung von RSA-3072 und ECC-256 mit NIST-Kurven)*

(5) [none]. [158]

Anwendungshinweis 104: Gemäß FMT_MOF.1/NK.TLS wird die Steuerung, unter welchen Umständen der Import von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen.

FDP_ETC.2/NK.TLS Export of user data with security attributes

Export von Zertifikaten

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

nicht erfüllt mit folgender Begründung: Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanagt. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen erzeugt und exportiert werden. Damit wird diese Abhängigkeit inhaltlich erfüllt.

FDP_ETC.2.1/NK.TLS The TSF shall enforce the *Certificate-Export-SFP*[159] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/NK.TLS The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/NK.TLS The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/NK.TLS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) Die TSF exportiert X.509 Zertifikate für Clientsysteme und den zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle. Als Exportformat wird PKCS#12 verwendet.

(2) [Die TSF exportiert X.509 Zertifikate für die Authentisierung des EVG bei TLS-Verbindungen zu Clientsystemen durch den Administrator über die Managementschnittstelle.]

[158] *[assignment: additional importation control rules].*

[159] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

(3) Die TSF generiert ein starkes Passwort zur Sicherung der PKCS#12 Datei, bietet dieses dem Administrator zur Verwendung an und akzeptiert beliebige vom Administrator selbst gewählte Passwörter.

(4) Die TSF prüft im Fall der Verwendung eines frei gewählten Passworts dessen Länge und Komplexität und zeigt dem Administrator Hinweise dazu an. [160]

Anwendungshinweis 105: Gemäß FMT_MOF.1/NK.TLS wird die Steuerung, unter welchen Umständen der Export von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen. Gem. TIP1-A_4517-04 erzwingt der EVG nicht die Nutzung eines starken Passworts zur Sicherung der PKCS#12-Datei.

FMT_MOF.1/NK.TLS Management of security functions behaviour

Management von TLS-Verbindungen durch den Anwendungskonnektor

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch FMT_SMR.1/NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch FMT_SMF.1/NK

FMT_MOF.1.1/NK.TLS The TSF shall restrict the ability to determine the behaviour of[161] the functions *Management of TLS-Connections required by the Anwendungskonnektor*[162] to *Anwendungskonnektor*[163].

The following rules apply: For each TLS-Connection managed by the Anwendungskonnektor, only the Anwendungskonnektor can determine:

1. **Whether one or both endpoints of the TLS-connection need to be authenticated and which authentication mechanism is used for each endpoint.**
2. **Whether the Konnektor or the remote IT-Product or both can initiate the TLS-Connection.**
3. **Whether TLS 1.2 or TLS 1.3 (if provided) are used and which subset of the set of cipher suites as listed in FTP_ITC.1/NK.TLS is allowed for each connection.**

[160] *[assignment: additional exportation control rules]*

[161] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[162] [assignment:*list of functions*]

[163] [assignment: *the authorised identified roles*]

4. **Whether a "Keep-Alive" mechanism is used for a connection.**
5. **Which data can or must be transmitted via each TLS-Connection.**
6. **Whether the validity of the certificate of a remote IT-Product needs to be verified and whether a certificate chain or a whitelist is used for this verification.**
7. **Under which conditions a TLS-connection is terminated.**
8. **Whether and how terminating and restarting a TLS-connection using a Session-ID is allowed.**
9. **Whether and under which conditions certificates and keys for TLS-Connections are generated and exported or imported.**
10. **[*none*]** [164]

If one or more of these rules are managed by the EVG itself, this shall also be interpreted as a fulfillment of this or these rules. [165]

Anwendungshinweis 106: Dieses SFR soll dafür sorgen, dass der Anwendungskonnektor alle Regeln durchsetzen kann, die gemäß der gematik-Spezifikationsdokumente für die verschiedenen vom Konnektor benötigten TLS-Verbindungen durchgesetzt werden müssen. Der EVG unterstützt ausschließlich TLS Version 1.2.

Es wurden neben den Vorgaben des PPs keine weiteren Handlungsoptionen für den Anwendungskonnektor beschrieben.

Der Netzkonnektor nutzt TLS-Verbindungen auch zur Absicherung der lokalen Administrierung. Diese Verbindungen werden nicht im Sinne von FMT_MOF.1/NK.TLS gemanagt, sondern sind mit der Implementierung der Management-Schnittstelle festgelegt.

Erläuterung: Im Schutzprofil für den Konnektor werden diese Regeln durch verschiedene SFRs für den Anwendungskonnektor konkretisiert.

Anwendungshinweis 107: Das im SFR beschriebene Mangement der TLS Verbindungen erfolgt durch den Anwendungskonnektor.

6.3. Anforderungen an die Vertrauenswürdigkeit des EVG

Es wird die Vertrauenswürdigkeitsstufe **EAL3** erweitert um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.5 und ALC_FLR.2 (EAL3 erweitert um die Komponenten **AVA_VAN.5** und deren direkte und transitive Abhängigkeiten ADV_IMP.1, ADV_TDS.3, ADV_FSP.4 und ALC_TAT.1) gefordert. Daraus ergibt sich eine **Resistenz gegen hohes Angriffspotential**. Darüber hinaus wird **ALC_FLR.2** gefordert. Eine Erklärung für die gewählte EAL-Stufe findet sich in Abschnitt 6.6.

164 **[assignment: *additional rules*]**

165 refinement

Einige Anforderungen an die Vertrauenswürdigkeit (Assurance) werden wie in den folgenden Unterabschnitten beschrieben verfeinert.

6.3.1. Verfeinerung von ALC_DEL.1

ALC_DEL.1 wird wie folgt verfeinert:

Das Auslieferungsverfahren muss Schutz gegen das In-Umlauf-Bringen gefälschter Konnektoren bieten (sowohl während der Erstauslieferung als auch bedingt durch unbemerkten Austausch), siehe O.NK.EVG_Authenticity. Dies unterstützt die Verwendung der (in EAL3 bereits enthaltenen) Komponente ALC_DEL.1. Das Auslieferungsverfahren muss so ausgestaltet werden, dass das Ziel O.NK.EVG_Authenticity erfüllt wird.

Der Hersteller muss das Auslieferungsverfahren beschreiben. Die Beschreibung des Auslieferungsverfahrens muss zeigen, auf welche Weise das Auslieferungsverfahren (in Verbindung mit den Verfahren zur Inbetriebnahme) des EVGs sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

Der Evaluator muss die Beschreibung analysieren (*examine*), um festzustellen, dass sie beschreibt, auf welche Weise das Auslieferungsverfahren (in Verbindung mit den Verfahren zur Inbetriebnahme) des EVGs sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

6.3.2. Verfeinerungen von AGD_OPE.1

AGD_OPE.1 wird bzgl. der **Inbetriebnahme** wie folgt verfeinert:

Das Verfahren zur Inbetriebnahme muss Schutz gegen das In-Umlauf-Bringen gefälschter Konnektoren bieten (sowohl während der Erstauslieferung als auch bedingt durch unbemerkten Austausch), siehe O.NK.EVG_Authenticity. Dies unterstützt die Verwendung der (in EAL3 bereits enthaltenen) Komponente AGD_OPE.1. Das Verfahren zur Inbetriebnahme muss so ausgestaltet werden, dass das Ziel O.NK.EVG_Authenticity erfüllt wird.

Der Hersteller muss in seiner Benutzerdokumentation das Verfahren zur Inbetriebnahme des EVGs beschreiben. Diese Beschreibung muss zeigen, auf welche Weise das Verfahren zur Inbetriebnahme (in Verbindung mit dem Auslieferungsverfahren) sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

Der Evaluator muss die Beschreibung analysieren (*examine*), um festzustellen, dass sie beschreibt, auf welche Weise das Verfahren zur Inbetriebnahme (in Verbindung mit dem Auslieferungsverfahren) sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

AGD_OPE.1 wird bzgl. der **Administration der Paketfilter-Regeln** wie folgt verfeinert:

Die Benutzerdokumentation muss für den Administrator verständlich beschreiben, welche Paketfilter-Regeln er administrieren kann. Die Benutzerdokumentation muss den Administrator befähigen, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu

konfigurieren. Für die von ihm administrierbaren Paketfilter-Regeln muss er in die Lage versetzt werden, geeignete Regelsätze aufzustellen.

Der Hersteller muss in seiner Benutzerdokumentation beschreiben, welche Paketfilter-Regeln der Administrator administrieren kann. Die Benutzerdokumentation muss den Administrator befähigen, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu konfigurieren. Für die von ihm administrierbaren Paketfilter-Regeln muss er in die Lage versetzt werden, geeignete Regelsätze aufzustellen.

Der Evaluator muss die Benutzerdokumentation analysieren (*examine*), um festzustellen, dass sie beschreibt, welche Paketfilter-Regeln der Administrator administrieren kann, und dass sie den Administrator befähigt, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu konfigurieren (für die von ihm administrierbaren Paketfilter-Regeln muss der Administrator in die Lage versetzt werden, geeignete Regelsätze aufzustellen).

AGD_OPE.1 wird bzgl. der **Internet-Anbindung** wie folgt verfeinert:

Die Benutzerdokumentation muss die Benutzer und Betreiber des Konnektors über die Risiken aufklären, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. das Internet erfolgt.

Der Hersteller muss in der Benutzerdokumentation die Benutzer und Betreiber des Konnektors über die Risiken aufklären, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. Internet erfolgt. Zudem muss der Hersteller in der Benutzerdokumentation verständlich darauf hinweisen, dass auch Angriffe aus dem Internet über SIS nicht auszuschließen sind. Das Client-System muss entsprechende Sicherheitsmaßnahmen besitzen.

Der Evaluator muss die Benutzerdokumentation analysieren (*examine*), um festzustellen, dass sie die Benutzer und Betreiber des Konnektors hinreichend gut (verständlich und vollständig) über die Risiken aufklärt, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. Internet erfolgt.

6.3.3. Verfeinerung von ADV_ARC

ADV_ARC.1 wird wie folgt verfeinert:

Die Sicherheitsarchitektur muss beschreiben, wie der EVG Daten, Kommunikationspfade und Zugriffe der unterschiedlichen Dienste und Anwendungen separiert.

Der Hersteller muss die Sicherheitsarchitektur beschreiben. Die Beschreibung der Sicherheitsarchitektur muss zeigen, auf welche Weise die Sicherheitsarchitektur des EVGs die Separation der unterschiedlichen Dienste und Anwendungen (zwischen LAN und WAN sowie zwischen den Updatemechanismen und dem Datenfluss im Normalbetrieb) sicherstellt.

Der Evaluator muss die Beschreibung analysieren (*examine*), um festzustellen, dass sie beschreibt, auf welche Weise die Sicherheitsarchitektur des EVGs die Separation der unterschiedlichen Dienste und Anwendungen sicherstellt.

6.4. Erklärung der Sicherheitsanforderungen (Security Requirements Rationale)

Dieser Abschnitt ist von PP [11] übernommen mit den Anpassungen bzgl. Software-Update und Konnektor-Management wie in Abschnitt 4.1.1 dargestellt. Alle hier dargestellten Informationen sind daher in sich konsistent.

6.4.1. Abbildung der EVG-Ziele auf Sicherheitsanforderungen

Tabelle 8 im folgenden Abschnitt 6.4.1.1 stellt die Abbildung der EVG-Ziele auf Sicherheitsanforderungen zunächst tabellarisch im Überblick dar. In Abschnitt 6.4.1.2 wird die Abbildung erläutert und die Erfüllung der Sicherheitsziele durch die Anforderungen begründet.

6.4.1.1. Überblick

Sicherheitsanforderung an den EVG	O.NK.TLS **Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Admin_Auth	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FTP_ITC.1/NK.VPN_TI									X		X	X			
FTP_ITC.1/NK.VPN_SIS									X		X	X			
FDP_IFC.1/NK.PF													X	X	X
FDP_IFF.1/NK.PF													X	X	X
FMT_MSA.3/NK.PF													X	X	
FPT_STM.1/NK						X	X								
FPT_TDC.1/NK.Zert										X					
FDP_RIP.1/NK		X													
FPT_TST.1/NK		X													
FPT_EMS.1/NK		X									X	X			
FAU_GEN.1/NK.SecLog						X									
FAU_GEN.2/NK.SecLog						X									
FMT_SMR.1/NK	X			X	X								X	X	
FMT_MTD.1/NK				X											
FIA_UID.1/NK.SMR				X											
FTP_TRP.1/NK.Admin	X			X	X										
FMT_SMF.1/NK				X									X	X	
FMT_MSA.1/NK.PF				X									X	X	
FMT_MSA.4/NK				X	X										
FCS_COP.1/NK.Hash		X										X			
FCS_COP.1/NK.HMAC												X			
FCS_COP.1/NK.Auth			X						X						
FCS_COP.1/NK.ESP											X				
FCS_COP.1/NK.IPsec											X				

Sicherheitsanforderung an den EVG	O.NK.TLS **Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Admin_Auth	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FCS_CKM.1/NK		X	X						X		X	X			
FCS_CKM.2/NK.IKE									X		X	X			
FCS_CKM.4/NK	X	X	X						X		X	X			
FTP_ITC.1/NK.TLS	X				X										
FPT_TDC.1/NK.TLS.Zert	X														
FCS_CKM.1/NK.TLS	X														
FCS_COP.1/NK.TLS.HMAC	X														
FCS_COP.1/NK.TLS.AES	X														
FCS_COP.1/NK.TLS.Auth	X														
FCS_CKM.1/NK.Zert	X														
FDP_ITC.2/NK.TLS	X														
FDP_ETC.2/NK.TLS	X														
FMT_MOF.1/NK.TLS	X														
FDP_ACC.1/NK.Update								X							
FDP_ACF.1/NK.Update								X							
FTP_ITC.1/NK.KSR								X							
FDP_UIT.1/NK.Update								X							

Tabelle 8: Abbildung der EVG-Ziele auf Sicherheitsanforderungen

6.4.1.2. Erfüllung der Sicherheitsziele durch die Anforderungen

In diesem Abschnitt wird erklärt, warum die Kombination der individuellen funktionalen Sicherheitsanforderungen (SFR) und Anforderungen an die Vertrauenswürdigkeit (SAR) für den EVG gemeinsam die formulierten Sicherheitsziele erfüllen.

Dazu wird in der folgenden Tabelle 9 jedes EVG-Ziel in einzelne Teilaspekte zerlegt, die dann auf Sicherheitsanforderungen abgebildet werden.[166] Um die Abbildung zu erklären (im Sinne des von Common Criteria geforderten Erklärungsteils / Rationale), wird in der Tabelle zu jeder solchen Abbildung eines Aspekts in der folgenden Zeile eine Begründung gegeben. Die Begründung zitiert, wo dies möglich ist, Sätze aus dem entsprechenden EVG-Ziel. Solche Zitate sind durch Anführungszeichen und Kursivschrift gekennzeichnet.

Grundsätzlich gilt, dass die korrekte Umsetzung eines Ziel in Sicherheitsanforderungen durch die im CC Teil 2 [2] aufgeführten Abhängigkeiten zwischen funktionalen Sicherheits-anforderungen (SFRs) unterstützt wird: Häufig lässt sich leicht ein SFR finden, welches

[166] Hinweis: Common Criteria fordert nur eine Abbildung der EVG-Ziele auf funktionale Sicherheitsanforderungen (SFRs). Es zeigte sich aber, dass auch Anforderungen an die Vertrauenswürdigkeit (SARs) bzw. deren Verfeinerungen einen Beitrag zum Erreichen der Sicherheitsziele leisten

wesentliche Aspekte des EVG-Ziels umsetzt. Betrachtet man alle Abhängigkeiten, so ergibt sich eine vollständige Abdeckung des EVG-Ziels. In der folgenden Tabelle werden daher abhängige SFRs ebenfalls mit aufgelistet. Dabei wird davon ausgegangen, dass die Abhängigkeit selbst nicht gesondert erläutert werden muss.

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
O.NK.TLS_Krypto	TLS-Kanäle	FTP_ITC.1/NK.TLS FMT_MOF.1/NK.TLS FMT_SMR.1/NK FMT_SMF.1/NK FPT_TDC.1/NK.TLS.Zert
	Begründung: In O.NK.TLS_Krypto wird gefordert: *„Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung“* Genau dies leistet FTP_ITC.1/NK.TLS. Mit FMT_MOF.1/NK.TLS wird der Rolle Anwendungskonnektor die Möglichkeit gegeben die TLS-Verbindungen zu Managen und je nach Anwendungsfall einzurichten. FMT_SMF.1/NK definiert diese Funktionalität und FMT_SMR.1/NK definiert diese Rolle (Anwendungskonnektor). Zertifikate die im Rahmen von TLS-Verbindungen zum Einsatz kommen werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.	
	Kommunikation mit anderen IT-Produkten	FCS_CKM.1/NK.Zert FCS_CKM.4/NK FDP_ITC.2/NK.TLS FTP_TRP.1/NK.Admin FDP_ETC.2/NK.TLS
	Gültigkeitsprüfung von Zertifikaten	FPT_TDC.1/NK.TLS.Zert
	Begründung: Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der EVG das exportieren von X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle (FDP_ETC.2/NK.TLS). Entsprechende Zertifikate können vom EVG durch die in FCS_CKM.1/NK.Zert geforderten Mechanismen erzeugt werden, FCS_CKM.4/NK unterstützt als abhängige Komponente. Zertifikate für Clientsysteme können auch vom EVG gemäß FDP_ITC.2/NK.TLS über die gesicherte Management-Schnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Die importierten Zertifikate werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert. Dabei wird auch eine Gültigkeitsprüfung der Zertifikate durchgeführt.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	sichere kryptographische Algorithmen und Protokolle	FCS_CKM.1/NK.TLS FCS_COP.1/NK.TLS.HMAC FCS_COP.1/NK.TLS.AES FCS_COP.1/NK.TLS.Auth FCS_CKM.4/NK
	Begründung: Für die TLS-Kanäle sind nach O.NK.TLS_Krypto nur „*sichere kryptographische Algorithmen und Protokolle gemäß [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [18]*“ zugelassen. FCS_COP.1/NK.TLS.Auth die unterstützt die Authentisierung im Rahmen des TLS-Verbindungsaufbaus, indem der dazu zu verwendende Algorithmus spezifiziert wird. FCS_COP.1/NK.TLS.HMAC spezifiziert die HMAC Algorithmen, die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen. Nach erfolgreichem Verbindungsaufbau wird die Kommunikation mit AES gemäß FCS_COP.1/NK.TLS.AES abgesichert. FCS_CKM.1/NK.TLS fordert, dass entsprechendes Schlüsselmaterial generiert wird, FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Schutz	Speicheraufbereitung: temporäre Kopien nicht mehr benötigter Geheimnisse werden unmittelbar nach Gebrauch aktiv überschrieben	FDP_RIP.1/NK
	Begründung: In O.NK.Schutz wird gefordert: „*Der EVG löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden.*“ Genau dies leistet FDP_RIP.1/NK. Auch die Zuweisung „upon the *deallocation of the resource from*“ passt zur Forderung in O.NK.Schutz. Die „*Geheimnisse (z. B. Schlüssel)*“ werden im SFR durch die Zuweisung präzisiert.	
	Selbsttests, Schutz gegen sicherheitstechnische Veränderungen	FPT_TST.1/NK
	Begründung: „*Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten:*“ → ist als Erläuterung für die Begriffsbildung O.NK.Schutz und als Oberbegriff für die weiteren Teilaspekte zu verstehen.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	„*Der EVG schützt sich selbst gegen sicherheitstechnische Veränderungen an den äußeren logischen Schnittstellen bzw. erkennt diese oder macht diese erkennbar. Der EVG erkennt bereits Versuche, sicherheitstechnische Veränderungen durchzuführen, sofern diese über die äußeren Schnittstellen des EVGs erfolgen (mit den unter OE.NK.phys_Schutz formulierten Einschränkungen). Der EVG führt beim Start-up und bei Bedarf Selbsttests durch.*“ → Das Erkennen bzw. Erkennbarmachen sicherheitstechnischer Veränderungen erfolgt durch den von FPT_TST.1/NK geforderten Selbsttest. Im Rahmen der Integritätsprüfungen werden Hashwerte wie von FCS_COP.1/NK.Hash gefordert verwendet. Dieses SFR hat die formalen Abhängigkeiten FCS_CKM.4/NK und FCS_CKM.1/NK, wobei FCS_CKM.4/NK nicht erfüllt werden muss, sofern im Rahmen der Hashwertberechnung keine geheimen Schlüssel verwendet werden. FCS_CKM.1/NK fordert, dass das Schlüsselmaterial (z. B. Integritätsprüfschlüssel) generiert wird. Anmerkung: Alternativ könnte ein Hersteller diese Schlüssel auch importieren; dazu wäre dann zusätzlich FDP_ITC.1 oder FDP_ITC.2 aufzunehmen.	
	Schutz gegen unbefugte Kenntnisnahme (Side Channel-Analysen)	FPT_EMS.1/NK
	Begründung: „*Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten.*“ Um den Aspekt „*die ihm anvertrauten Benutzerdaten*“ vollständig abzudecken, wurde die explizite Komponente FPT_EMS.1/NK ergänzt. Dieses SFR fordert genau die Analyse, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen.	
O.NK.Stateful	dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	FDP_IFC.1/NK.PF → FDP_IFF.1/NK.PF
	Begründung: „*Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter.*“ Diese Paketfilterung wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF). Die zustandsgesteuerte Filterung wurde in den Operationen und im Refinement zu FDP_IFF.1/NK.PF modelliert.	
O.NK.EVG_Authenticity	Auslieferungsverfahren: Nur authentische EVGs können in Umlauf gebracht werden	FCS_COP.1/NK.Auth FCS_CKM.1/NK FCS_CKM.4/NK

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	Begründung: „*Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können. Gefälschte EVGs müssen vom VPN-Konzentrator sicher erkannt werden können. Der EVG muss auf Anforderung mit Unterstützung der SM NK einen Nachweis seiner Authentizität ermöglichen.*“ → Die Authentisierung wird mit Kryptoalgorithmen erbracht, die durch FCS_COP.1/NK.Auth spezifiziert werden. FCS_CKM.1/NK fordert eine Generierung des für den Nachweis der Authentizität des EVGs erforderlichen Schlüsselmaterials; FCS_CKM.4/NK unterstützt als abhängige Komponenten dabei.	
O.NK.Admin_EVG	rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen	FMT_MTD.1/NK FMT_SMR.1/NK FMT_SMF.1/NK
	Identifikation / Autorisierung des Administrators	FIA_UID.1/NK.SMR FMT_MSA.4/NK
	sicherer Pfad	FTP_TRP.1/NK.Admin
	Beschränkung der Administration der Firewall-Regeln	FMT_MSA.1/NK.PF
	Begründung: „*Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen.*“ → FMT_MTD.1/NK beschränkt den Zugriff wie vom Ziel gefordert auf die Rolle Administrator. FMT_SMR.1/NK modelliert als abhängige Komponente diese Rolle (Administrator). FIA_UID.1/NK.SMR erfordert eine Identifikation des Benutzers vor jeglichem Zugriff auf administrative Funktionalität. Die Menge der administrativen Funktionen wird in FMT_SMF.1/NK aufgelistet. „*Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung eines Administrators, welcher die lokale und entfernte Administration des EVG durchführen kann.*“ → Die Authentisierung des Administrators erfolgt durch den EVG selbst. Nach erfolgreicher Authentisierung wird ein Sicherheitsattribut gesetzt. Die dabei anzuwendenden Regeln wurden in FMT_MSA.4/NK modelliert. „*Die Administration erfolgt rollenbasiert.*“ → FMT_SMR.1/NK modelliert die Rolle Administrator. „*Weil die Administration über Netzverbindungen (lokal über PS2 oder zentral über PS3) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).“ → FTP_TRP.1/NK.Admin fordert genau diesen sicheren logischen Kanal zum Benutzer (trusted path). „*Der EVG verhindert die Administration folgender Firewall-Regeln: …*“ → Dieser Aspekt wird durch das Refinement zu FMT_MSA.1/NK.PF abgebildet. Schließlich unterstützt die Benutzerdokumentation (AGD_OPE.1) bei der Administration der Paketfilter-Regeln.	
O.NK.Admin_Auth	Der Netzkonnektor führt die Authentisierung des Administrators durch.	FMT_SMR.1/NK FTP_TRP.1/NK.Admin FMT_MSA.4/NK FTP_ITC.1/NK.TLS FTP_ITC.1.1/NK.VPN_SIS
	Begründung: FMT_SMR.1/NK modelliert die Rolle des Administrators. FTP_TRP.1/NK.Admin fordert einen sicheren Kommunikationskanal zwischen EVG und Administrator, sowohl für lokale als auch für entfernte Administrierung. Der sichere Kanal wird durch FTP_ITC.1/NK.TLS umgesetzt, in dem ein sicherer TLS-Kanal für lokale und entfernte Administrierung gefordert wird. Die Kryptografischen Basisdienste werden dabei von O.NK.TLS_Krypto umgesetzt. Für entfernte Administrierung ist zu dem eine VPN Verbindung notwendig, diese wird durch FTP_ITC.1.1/NK.VPN_SIS umgesetzt. Erst nach erfolgreicher Authentisierung wird ein entsprechender Autorisierungsstatus im EVG gesetzt (FMT_MSA.4/NK).	
O.NK.Protokoll	EVG protokolliert sicherheitsrelevante Ereignisse mit Daten und Zeitstempel	FAU_GEN.1/NK.SecLog FAU_GEN.2/NK.SecLog FPT_STM.1/NK
	Begründung: „*Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit.“* → FAU_GEN.1/NK.SecLog fordert eine Protokollierung für die in der Operation explizit aufgelisteten Ereignisse und stellt Anforderungen an den Inhalt der einzelnen Log-Einträge. FAU_GEN.2/NK.SecLog fordert, dass die Benutzeridentitäten mit protokolliert werden. FPT_STM.1/NK stellt den Zeitstempel bereit.	
O.NK.Zeitdienst	regelmäßige Zeitsynchronisation	FPT_STM.1/NK
	Begründung:	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	„*Der EVG synchronisiert die Echtzeituhr gemäß OE.NK*.Echtzeituhr *in regelmäßigen Abständen über einen sicheren Kanal mit einem vertrauenswürdigen Zeitdienst (siehe OE.NK*.Zeitsynchro*).*“ → (Refinement zu) FPT_STM.1/NK: Synchronisation mindestens einmal innerhalb von 24 Stunden; Information, falls die Synchronisierung nicht erfolgreich durchgeführt werden konnte	
O.NK.Update	Integrität und Authentizität des Software Update durch Administrator	FDP_ACC.1/NK.Update FDP_ACF.1/NK.Update FTP_ITC.1/NK.KSR FDP_UIT.1/NK.Update
	Begründung: Das Sicherheitsziel O.NK.Update fordert vom EVG die Möglichkeit Software-Komponenten zu aktualisieren. Die Updatedaten müssen vorher durch den EVG auf Integrität und Authentizität sowie auf Zulässigkeit der Updatedaten und Metadaten geprüft werden. FDP_ACC.1/NK.Update definiert die Update-SFP für solche Updates und FDP_ACC.1/NK.Update gibt die Regeln für den Umgang mit dem Software-Update beim Import vor. Die Anforderung FTP_ITC.1/NK.KSR fordert, dass der EVG Software-Komponenten von über einen sicheren Kanal vom KSR-Server importieren kann. Mit FDP_UIT.1/NK.Update wird die Prüfung der Integrität dieser Daten vor dem Update gefordert.	
O.NK.VPN_Auth	gegenseitige Authentisierung mit VPN-Konzentrator (Telematikinfrastruktur-Netz)	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Auth → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK
	Begründung: FCS_COP.1/NK.Auth setzt direkt die Anforderung nach einer Authentisierung des EVGs gegenüber dem VPN-Konzentrator um, indem es die dazu zu verwendenden Algorithmen spezifiziert. FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS fordern die sicheren Kanäle mit gegenseitiger Authentisierung („ … provides assured identification of its end points …“) zu den VPN-Konzentratoren in die Telematikinfrastruktur bzw. ins Internet. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS (IPsec) und FCS_CKM.2/NK.IKE (IKE) legen fest, welche Protokolle im Rahmen des Kanalaufbaus verwendet werden sollen. Zwar geht es in	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	FCS_CKM.2/NK.IKE vorrangig um die Schlüsselableitung, diese ist aber mit der Authentisierung kombiniert. FCS_CKM.1/NK fordert, dass entsprechendes Schlüsselmaterial für die Authentisierung generiert wird (evtl. unter Rückgriff auf eine gSMC-K, welches in den EVG eingebracht wird). FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Zert_Prüf	Gültigkeitsprüfung von Zertifikaten mit Hilfe von TSL und der CRL	FPT_TDC.1/NK.Zert
	Begründung: Zertifikatsprüfung: „*Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form einer zugehörigen CRL und einer TSL bereitgestellt.*“ FPT_TDC.1/NK.Zert fordert, dass der EVG Informationen über die Gültigkeit von Zertifikaten korrekt interpretiert. In der Zuweisung wurden TSL und CRL explizit erwähnt: „*The TSF shall provide the capability to consistently interpret information – distributed in the form of a TSL (Trust-Service Status List) or CRL (Certificate Revocation List) information …*“ Die Zertifikatsprüfung wird für VPN-Konzentratoren der Telematikinfrastruktur-Netzes bzw. des Sicheren Internet Service durchgeführt. FPT_TDC.1/NK.Zert fordert ferner explizit, dass der EVG Informationen „*about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects”*interpretiert.	
O.NK.VPN_Vertraul	Vertraulichkeit der Nutzdaten im VPN (Telematikinfrastruktur-Netz) IPsec-Kanal: Ableitung von *session keys*, AES-Verschlüsselung mit den *session keys* , Zerstörung der *session keys* nach Verwendung, Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.IPsec, → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_COP.1/NK.ESP → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Vertraulichkeit der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren verschlüsselt (vor dem Versand) bzw. entschlüsselt (nach dem Empfang) der Konnektor die Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Verschlüsselung wird durch FTP_ITC.1/NK.VPN_TI (im Fall der Telematikinfrastruktur) bzw. FTP_ITC.1/NK.VPN_SIS (im Fall des Sicheren Internet Service) gefordert *(„ ...protection of the channel data from modification and disclosure“*, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.IPsec ermöglicht die Definition der zu verwendenden Verschlüsselungsalgorithmen, hier AES gemäß FCS_COP.1/NK.ESP. FCS_CKM.4/NK unterstützt als abhängige Komponente ebenfalls. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet. FCS_CKM.1/NK fordert eine solche Generierung von *session keys*. *„Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.“* → Mittels FCS_CKM.2/NK.IKE (IKE) werden die abgeleiteten Sitzungsschlüssel, die für die Verschlüsselung verwendet werden, mit der die Vertraulichkeit der Nutzdaten sichergestellt wird, mit der Gegenstelle ausgetauscht. Die Nutzdaten werden mit AES gemäß FCS_COP.1/NK.ESP verschlüsselt. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.VPN_Integrität	Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von *session keys*, Austausch der *session keys* mit Gegenstelle, Zerstörung der *session keys* nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von *session keys*, Zerstörung der *session keys* nach Verwendung Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Hash → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK FCS_COP.1/NK.HMAC → FCS_CKM.1/NK → FCS_CKM.4/NK FPT_EMS.1/NK

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	Begründung: „*Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.*“ → Die Integritätssicherung wird durch FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS gefordert („*...protection of the channel data from modification and disclosure*“, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Encapsulating Security Payload (ESP) (RFC 4303 (ESP), [30]) erfolgt, wobei die Authentizitätsdaten (authentication data) den Wert des Integritätstests (integrity check value) enthalten, der sich wiederum aus einem Hash über den ESP Header und den verschlüsselten Nutzdaten des Paketes ergibt. Insofern ist eine Hashfunktion erforderlich. Weiterhin ist im IPSec sowie in IKE Standard die Verwendung von HMAC Algorithmen enthalten ([34], [35], [31]). Dies wird durch FCS_COP.1/NK.HMAC erreicht. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet (FCS_CKM.1/NK) und mit der Gegenstelle ausgetauscht (FCS_CKM.2/NK.IKE). FCS_CKM.4/NK unterstützt als abhängige Komponente. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.PF_WAN	dynamischer Paketfilter zum WAN	FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, FMT_MSA.3/NK.PF, FMT_MSA.1/NK.PF, FMT_SMR.1/NK FMT_SMF.1/NK AVA_VAN.5 (hohes Angriffspotential)
	Begründung:	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	„*Der EVG schützt sich selbst, andere Konnektorteile und die Clientsysteme vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN).“* → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „*The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects VPN concentrator and attacker communicating with the TOE from its WAN interface (PS3) …*“ FDP_IFF.1/NK.PF modelliert einen Paketfilter („*…the decision shall be based on the following security attributes: IP address, port number, and protocol type.*“, „*For every operation (…) the TOE shall maintain a set of packet filtering rules …*“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (*Stateful Packet Inspection*) abgebildet und durch ein Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF (für die Paketfilterregeln im Allgemeinen). Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen (z. B Administrator) und verhindert so unbefugte Veränderungen an den sicherheitsrelevanten Filterregeln. FMT_SMR.1/NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf.	
O.NK.PF_LAN	dynamischer Paketfilter zum LAN, regelbasierte Informationsflusskontrolle	FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, FMT_MSA.3/NK.PF, FMT_MSA.1/NK.PF, FMT_SMR.1/NK FMT_SMF.1/NK FDP_IFF.1/NK.PF
	Begründung: „*Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN).“* → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF):	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	„*The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects … and the subjects application connector and workstation (German: Clientsystem) communicating with the TOE from its LAN interface (PS2) …*“ FDP_IFF.1/NK.PF modelliert einen Paketfilter („…*the decision shall be based on the following security attributes: IP address, port number, and protocol type.*“, „*For every operation (…) the TOE shall maintain a set of packet filtering rules …*“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (*Stateful Packet Inspection*) abgebildet und durch das folgende Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen. FMT_SMR.1/NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf. *„Für zu schützende Daten der TI und der Bestandsnetze sowie zu schützende Nutzerdaten bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Clientsystemen) auf das Transportnetz wird durch den EVG unterbunden: IT-Systeme im LAN können nur unter der Kontrolle des EVG und im Einklang mit der Sicherheitspolitik des EVG zugreifen.*“ → Dies wurde teilweise durch FDP_IFF.1.3/NK.PF modelliert (zwangsweise Nutzung des VPN-Tunnels). Ferner ist die Sicherheitsleistung des Paketfilters natürlich abhängig von den verwendeten Paketfilterregeln. Daher beschränkt der EVG die Administration gewisser grundlegender Paketfilterregeln; siehe dazu das Refinement zu FMT_MSA.1/NK.PF. Für die Paketfilterregeln, die der Administrator administrieren darf, informiert ihn die Benutzerdokumentation hinreichend; siehe dazu das Refinement zu AGD_OPE.1 (Administration der Paketfilter-Regeln) in Abschnitt 6.2.8.	

Tabelle 9: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 108: Hinweis zu O.NK.VPN_Integrität: Zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash werden nur Hashfunktionen verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruhen, entsprechend sind keine geheimzuhaltenden Schlüssel erforderlich.

6.4.2. Erfüllung der Abhängigkeiten

6.4.2.1. Erfüllung der funktionalen Anforderungen

In Abschnitt 6.1.1 wird für jede funktionale Anforderung die Menge aller von ihr abhängigen Komponenten unter dem Stichwort *Dependencies* aufgeführt. Die Erfüllung der Abhängigkeiten wird jeweils unter dem Stichwort *hier erfüllt durch:* demonstriert.

Wird eine Abhängigkeit nicht erfüllt, so wird unter dem Stichwort *Diese Abhängigkeit wird nicht erfüllt. Begründung:* diskutiert und begründet, weshalb die Abhängigkeit nicht erfüllt werden muss.

6.4.2.2. Erfüllung der Anforderungen an die Vertrauenswürdigkeit

Es wurde eine vollständige EAL-Stufe ausgewählt (EAL3) und anschließend augmentiert. Die EAL-Stufe an sich ist in sich konsistent und erfüllt alle Abhängigkeiten. Die Abhängigkeiten der im Rahmen der Augmentierung neu hinzugekommenen Komponenten (siehe Kapitel 2.3) werden ebenfalls erfüllt, wie die folgende Tabelle 10 zeigt.

Augmen-tierung	Abhängig-keit(en)	Bewertung	Erfüllung der Abhängigkeit?
AVA_VAN.5	ADV_ARC.1	ist Bestandteil von EAL3	Abhängigkeit ist erfüllt
	ADV_TDS.3	wird augmentiert	Abhängigkeit ist erfüllt
	ADV_FSP.4	wird augmentiert	Abhängigkeit ist erfüllt
	ADV_IMP.1	wird augmentiert	Abhängigkeit ist erfüllt
	AGD_OPE.1	ist Bestandteil von EAL3	Abhängigkeit ist erfüllt
	AGD_PRE.1	ist Bestandteil von EAL3	Abhängigkeit ist erfüllt
	ATE_DPT.1	ist Bestandteil von EAL3	Abhängigkeit ist erfüllt
ADV_TDS.3	ADV_FSP.4	wird augmentiert	Abhängigkeit ist erfüllt
ADV_FSP.4	ADV_TDS.1	ADV_TDS.2 ist Bestandteil von EAL3, ADV_TDS.1 ist enthalten in ADV_TDS.2;	Abhängigkeit ist erfüllt
ADV_IMP.1	ADV_TDS.3	wird augmentiert	Abhängigkeit ist erfüllt
	ALC_TAT.1	wird augmentiert (siehe Anmerkung)	Abhängigkeit ist erfüllt
ALC_TAT.1	ADV_IMP.1	wird augmentiert	Abhängigkeit ist erfüllt
ALC_FLR.2	keine		

Tabelle 10: Erfüllung der Abhängigkeiten der augmentierten Komponenten

Anmerkung: Die in CC Teil 3 [3] angegebenen Abhängigkeiten von AVA_VAN.5 sind leider nicht vollständig aufgelöst: ADV_IMP.1 impliziert zusätzlich ALC_TAT.1.

6.5. Erklärung für Erweiterungen

Dieses Security Target definiert neben den Vorgaben aus dem PP [11] keine weiteren Erweiterungen. Die Erklärung für Erweiterungen aus dem PP [11] gilt daher unverändert auch für dieses Security Target.

6.6. Erklärung für die gewählte EAL-Stufe

Dieses Security Target übernimmt die EAL Stufe mit Augmentierung aus dem PP [11]. Darüber hinaus wird keine weitere Augmentierung vorgenommen. Die Erklärung für Erweiterungen die gewählte EAL-Stufe aus dem PP [11] gilt daher unverändert auch für dieses Security Target.

7. Zusammenfassung der EVG Sicherheitsfunktionalität

Die funktionalen Sicherheitsanforderungen werden im Folgenden nach funktionalen Gruppen gegliedert. Die funktionalen Gruppen orientieren sich an den in Abschnitt 1.3.5 beschriebenen Sicherheitsdiensten und der Gliederung der Sicherheitsfunktionen in Abschnitt 6. Im Folgenden werden die Sicherheitsfunktionen kurz zusammengefasst:

- VPN-Client: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);
- Dynamischer Paketfilter: sowohl für WAN als auch für LAN;
- Netzdienste: Zeitsynchronisation über sicheren Kanal, Zertifikatsprüfung mittels Sperrlisten;
- Stateful Packet Inspection: Generierung von Audit-Daten für spätere zustandsgesteuerte Filterung;
- Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, optional sichere Kanäle zu anderen Komponenten des Konnektors, Protokollierung Sicherheits-Log;
- Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, eingeschränkte Möglichkeit der Administration von Firewall-Regeln.
- Kryptographische Basisdienste: Kryptographische Algorithmen für den Aufbau und die Verwendung von VPN/IPsec
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen: Kryptographische Algorithmen für TLS, Anforderungen an TLS-Kanäle, Prüfung von TLS-Zertifikaten. Management von TLS-Kanälen

7.1. Sicherheitsfunktionen des EVG

7.1.1. VPN-Client

VPN

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. Verbindungen zum *VPN-Konzentrator der Telematikinfrastruktur* werden entsprechend FTP_ITC.1/NK.VPN_TI umgesetzt. Verbindungen zum *Sicheren Internet Service (SIS)* werden entsprechend FTP_ITC.1/NK.VPN_SIS umgesetzt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei wird IKEv2 unterstützt.

Informationsflusskontrolle

Regelbasiert verwenden 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, verwenden den VPN-Tunnel zum Sicheren Internet Service.

Diese Aspekte ergeben aus der Betrachtung der VPN-Kanäle und werden mittels dynamischen Paketfilters umgesetzt (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, siehe dazu Abschnitt 7.1.2.

Durch FDP_IFF.1.2/NK.PF wird eine VPN-Nutzung für *zu schützende Daten der TI und der Bestandsnetze* und für *zu schützende Nutzerdaten* (im Sinne des Abschnitts 3.1) gefordert, sofern die Paketfilter-Regeln geeignet gesetzt sind.

7.1.2. Dynamischer Paketfilter

Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird als Informationsflusskontrolle modelliert (siehe FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF). Zur zustandsgesteuerten Filterung siehe auch Abschnitt 7.1.4 Stateful Packet Inspection.

Die von FDP_IFF.1.2/NK.PF geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (siehe unten, FMT_MSA.3/NK.PF) und können vom Administrator verwaltet werden (siehe FMT_MSA.1/NK.PF, vgl. Abschnitt 6.2.6 Administration).

7.1.3. Netzdienste

Zeitsynchronisation

Bei aktiviertem „Leistungsumfang Online“ (MGM_LU_ONLIONE=Enabled) führt der EVG in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Siehe auch Sicherheitsdienst Zeitdienst (siehe FPT_STM.1/NK). Kann eine Zeitsynchronisation innerhalb eines bestimmten Zeitraums nicht erfolgreich durchgeführt werden oder überschreitet die Zeitabweichung zwischen Systemzeit und Zeit des Zeitservers zum Zeitpunkt der Zeitsynchronisierung einen bestimmten Wert, so wird der kritische Betriebszustand an der Signaleinrichtung des Konnektors angezeigt.

Der Administrator kann die Zeit des Konnektors auch über das Managementinterface einstellen, falls MGM_LU_ONLINE nicht aktiv ist.

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 mittels der aktuell gültigen TSL und CRL (siehe FPT_TDC.1/NK.Zert).

7.1.4. Stateful Packet Inspection

Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“ (engl. „stateful packet inspection“ oder auch „stateful inspection“ genannt). 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.

Der Aspekt der Stateful Packet Inspection wird durch FDP_IFF.1.4/NK.PF modelliert.

7.1.5. Selbstschutz

Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren. Versuche, den ausführbaren Code zu verändern werden durch Prüfung der Integrität der installierten SW Images bei jedem Start (Secure Boot) gewährleistet (siehe Selbsttests).

Speicheraufbereitung

Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben mit Nullen oder festen Werten (siehe FDP_RIP.1/NK). 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.

Selbsttests

Der EVG bietet seinen Benutzern eine Möglichkeit, die eigene Integrität zu überprüfen (siehe FPT_TST.1/NK).

Bei Programmstart wird eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) durch Verifikation von Signaturen durchgeführt.

Das BIOS unterstützt Secure Boot nach der UEFI Spezifikation [21], Kapitel 30, „Secure Boot and Driver Signing“. Jeder extern nachgeladene UEFI Code kann nur ausgeführt werden, wenn die Signaturprüfung erfolgreich ist. Auf dem Konnektor kommt ein Customized BIOS zum Einsatz, das ausschließlich den Public Key des Konnektor-Herstellers enthält. Somit kann vom BIOS aus nur Code ausgeführt werden, der mit dem geheimen Schlüssel des Herstellers signiert wurde. Das UEFI verifiziert die Signatur des Bootloaders und führt diesen aus. Im nächsten Schritt wird die Signatur des Kernels vom Bootloader vor dessen Ausführung verifiziert. Der Kernel prüft die Signatur des Host-OS Images. Das Host-OS-Filesystem wird nur dann eingebunden, wenn die Signatur erfolgreich verifiziert werden konnte. Nach Einbinden des Host-OS-Images werden die Signaturen der einzelnen Images der virtuellen Maschinen auf korrektheit geprüft.

Mit diesem Prozess ist auch die Integrität der Implementierung kryptographischer Verfahren sichergestellt. Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K als Seed Quelle für den Zufallszahlengenerator des Betriebssystems. Dieser ist durch die Prüfung der Integrität ebenfalls vor Manipulationen abgesichert. Der Benutzer kann die Selbsttests durch Neustart des EVGs oder über das Management-Interface anstoßen.

Schlägt die Prüfung der Integrität fehl, so wird der start up Prozess abgebrochen. Nach einem Neustart wird der Prozess erneut durchlaufen.

Schutz von Geheimnissen, Seitenkanalresistenz

Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme einschließlich der Kenntnisnahme nach Angriffen durch Seitenkanal-Analysen (side channel analysis), siehe FPT_EMS.1/NK. Dies gilt grundsätzlich für *kryptographisches Schlüsselmaterial* (siehe Tabelle 5: Sekundäre Werte in Abschnitt 3.1.2).

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.

Sicherheits-Log

Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation [16], Abschnitt 4.1.10 wie unter Sicherheitsdienst *Protokollierung* in Abschnitt 1.3.5 beschrieben. Diese Funktionalität ist mit FAU_GEN.1/NK.SecLog und FAU_GEN.2/NK.SecLog modelliert.

7.1.6. Administration

Administrator-Rollen, Management-Funktionen, Authentisierung der Administratoren, gesicherte Wartung

Der EVG verwaltet eine Administrator-Rolle (FMT_SMR.1/NK). Der Administrator muss autorisiert sein (FIA_UID.1/NK.SMR, FMT_SMR.1/NK und FMT_MSA.4/NK), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1/NK). Die Authentisierung erfolgt dabei durch den Netzkonnektor selbst.

Erst nach erfolgreicher Authentisierung wird ein entsprechender Autorisierungsstatus im EVG gesetzt (FMT_MSA.4/NK).

Die Wartung selbst erfolgt unter der Annahme, dass der Administrator über Netzwerkverbindungen (z. B. LAN, WAN) zugreift, stets über eine sichere TLS Verbindung (siehe FTP_TRP.1/NK.Admin). Der sichere TLS-Kanal wird durch FTP_ITC.1/NK.TLS umgesetzt. Die entfernte Administrierung kann über VPN-SIS oder direkt über das Internet erfolgen. Die TLS-Verbindung wird mit einem Herstellerspezifischen Schlüssel, der im Sicherheitsmodul gSMC-K abgelegt ist, aufgebaut (FCS_COP.1/NK.TLS.Auth). Über die TLS

Verbindung können HTTP Requests an die Management Schnittstelle gesendet werden. Die Management-Schnittstelle ist als REST-Schnittstelle implementiert.

Die administrativen Tätigkeiten bzw. Wartungstätigkeiten werden in FMT_SMF.1/NK aufgelistet. Dazu gehören die Verwaltung der Filterregeln für den dynamischen Paketfilter sowie das Aktivieren und Deaktivieren des VPN-Tunnels.

Die Administration der Filterregeln für den dynamischen Paketfilter (siehe: FDP_IFC.1/NK.PF) ist den Administratoren vorbehalten (FMT_MSA.1/NK.PF).

Software Update

Der Upate-Dienst des EVG kann über einen sicheren Kanal beim zentralen Konfigurationsdienst der TI (FTP_ITC.1/NK.KSR) Informationen über verfügbare Update-Pakete erhalten und automatisch oder manuell (durch den Administrator) in den vorgesehenen Speicherbereich laden. Alternativ kann auch über die lokale Management-Schnittstelle ein Update-Paket bezogen werden (FTP_TRP.1/NK.Admin). Der Administrator wird informiert, wenn ein neues Update-Paket auf dem RISE-Konnektor vorliegt. Der Administrator kann daraufhin nach erfolgreicher Signaturprüfung des Update-Paketes die Integrität (FDP_UIT.1/NK.Update) und Version prüfen und den Updateprozess anstoßen (FDP_ACC.1/NK.Update). Der EVG stellt sicher, dass Software Updates durch den lokalen Administrator freigeschaltet werden (FDP_ACF.1/NK.Update). Die Updates der Software des Konnektors können auch automatisch installiert werden, wenn dies explizit vom Administrator so konfiguriert wurde (FMT_MTD.1/NK).

Im Falle einer Software-Aktualisierung wird das aktuelle integere Software Image im EVG als „Fallback-Image“ beibehalten. Nach erfolgreicher Signaturprüfung des Update-Paketes wird das neue Software Image installiert. Erst wenn die Installation efolgreich abgelaufen ist, wird das neue Image aktiviert und ein Neustart durchgeführt. Schlägt die Signaturprüfung fehl oder kommt es während der Bootvorgangs zu Fehlern, wird das Update-Paket verworfen und das Fallback-Image wiederhergestellt. Nach erfolgreichem Neustart wird das Fallback-Image verworfen. Durch diesen Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können (FDP_UIT.1/NK.Update).

7.1.7. Kryptographische Basisdienste

Der Konnektor implementiert gemäß der Vorgaben des Dokuments „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt]“ [18] die im Folgenden aufgelistete kryptographischen Primitive:

Der Konnektor Unterstützt Hash-Berechnung (FCS_COP.1/NK.Hash) und HMAC-Berechnung (FCS_COP.1/NK.HMAC) im Rahmen des Aufbaus von VPN Verbindungen. Die Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256 und RSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen (siehe FCS_COP.1/NK.Auth) wird vom Netzkonnektor mit Hilfe der *gSMC-K* durchgeführt.

Die Absicherung des IPsec-Tunnels erfolgt durch Ver- und Entschlüsselung mittels symmetrischer Algorithmen (AES im CBC Modus mit 256 Bit Schlüssellänge), siehe

FCS_COP.1/NK.ESP. VPN Kommunikation erfolgt dabei nach dem IPsec Protocol (FCS_COP.1/NK.IPsec)

Die Schlüssel für die VPN-Kanäle werden mit hoher Qualität erzeugt (FCS_CKM.1/NK). Die Schlüsselerzeugung erfolgt für alle oben benannten kryptographischen Algorithmen (FCS_COP.1/NK.HMAC, FCS_COP.1/NK.Auth, FCS_COP.1/NK.ESP, FCS_COP.1/NK.IPsec). Der Schlüsselaustausch zum Aufbau von VPN-Tunnel erfolgt nach IPsec IKEv2, siehe FCS_CKM.2/NK.IKE. Nicht mehr benötigte Schlüssel werden sofort vernichtet, siehe FCS_CKM.4/NK. Diese werden aktiv mit Nullen überschrieben.

Die kryptographischen Basisdienste (z.B. Hash-Berechnung, AES Ver-/Entschlüsselung) des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des VPN Kanals).

7.1.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Der Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung (FTP_ITC.1/NK.TLS). Dabei wird die TLS Funktionalität dem Anwendungskonnektor zur Verfügung gestellt der auch das Management der TLS Verbindung übernimmt (FMT_MOF.1/NK.TLS). Zertifikate die während des Aufbaus einer TLS-Verbindung zur Authentisierung verwendet werden, werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.

Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der Netzkonnektor das exportieren von X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle (FDP_ETC.2/NK.TLS). Der Netzkonnektor bietet dabei die Möglichkeit solche Zertifikate und entsprechende RSA Schlüsselpaare zu erzeugen (FCS_CKM.1/NK.Zert). Die RSA Schlüssel werden nach dem Export durch das überschreiben mit festen Werten im EVG gelöscht (FCS_CKM.4/NK)

Zertifikate und Schlüsselmaterial für die Anbindung der Clientsysteme können auch vom EVG gemäß FDP_ITC.2/NK.TLS über die gesicherte Management-Schnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Diese werden beim Import nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert. Darüber hinaus werden die Zertifikate für NK.VPN, AK.AUT, SAK.AUT, SAK.AUTD_CVC und CA_SAK.CS im Rahmen der Laufzeitverlängerung gSMC-K abhängig von der vom Administrator gewählten Einstellung automatisch oder manuell importiert und im sicheren Datenspeicher abgelegt.

Für die TLS-Kanäle werden die sicheren kryptographische Algorithmen und Protokolle gemäß [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [18] implementiert.

Der Konnektor Unterstützt HMAC-Berechnung (FCS_COP.1/NK.TLS.HMAC) im Rahmen des Aufbaus von TLS Verbindungen. Die Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256 und RSA/ECDSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen (siehe FCS_COP.1/NK.TLS.Auth) wird vom Netzkonnektor mit Hilfe der *gSMC-K* oder *SMC-B* durchgeführt. Der EVG unterstützt ausschließlich sha256withRSAEncryption oder ecdsa-with-SHA256.

Nach erfolgreichem Verbindungsaufbau wird die Kommunikation mit AES gemäß FCS_COP.1/NK.TLS.AES abgesichert. Die Schlüssel für die TLS-Kanäle werden mit hoher Qualität erzeugt (FCS_CKM.1/NK.TLS). Nicht mehr benötigte Schlüssel werden sofort vernichtet, siehe FCS_CKM.4/NK. Diese werden aktiv mit Nullen überschrieben.

7.2. Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen

Tabelle 11 im folgenden Abschnitt 7.2.1 stellt die Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen zunächst tabellarisch im Überblick dar. In Abschnitt 7.2.2 wird die Abbildung erläutert und die Umsetzung der Anforderungen durch die Sicherheitsfunktionalität begründet.

7.2.1. Überblick

Sicherheitsanforderung an den EVG	7.1.1 **VPN-Client**	7.1.2 **Dynamischer Paketfilter**	7.1.3 **Netzdienste**	7.1.4 **Stateful Packet Inspection**	7.1.5 **Selbstschutz**	7.1.6 **Administration**	7.1.7 **Kryptographische Basisdienste**	7.1.8 **TLS-Kanäle unter Nutzung sicherer kryptographischer**
FTP_ITC.1/NK.VPN_TI	X							
FTP_ITC.1/NK.VPN_SIS	X							
FDP_IFC.1/NK.PF		X						
FDP_IFF.1/NK.PF		X		X				
FMT_MSA.3/NK.PF		X						
FMT_MSA.1/NK.PF		X						
FPT_STM.1/NK			X					
FPT_TDC.1/NK.Zert			X					
FDP_RIP.1/NK					X			
FPT_TST.1/NK					X			
FPT_EMS.1/NK					X			
FAU_GEN.1/NK.SecLog					X			
FAU_GEN.2/NK.SecLog					X			
FMT_SMR.1/NK						X		
FMT_MTD.1/NK						X		
FIA_UID.1/NK.SMR						X		
FTP_TRP.1/NK.Admin						X		
FMT_SMF.1/NK						X		
FMT_MSA.4/NK						X		
FCS_COP.1/NK.Hash							X	
FCS_COP.1/NK.HMAC							X	
FCS_COP.1/NK.Auth							X	
FCS_COP.1/NK.ESP							X	
FCS_COP.1/NK.IPsec							X	

Sicherheitsanforderung an den EVG	7.1.1 **VPN-Client**	7.1.2 **Dynamischer Paketfilter**	7.1.3 **Netzdienste**	7.1.4 **Stateful Packet Inspection**	7.1.5 **Selbstschutz**	7.1.6 **Administration**	7.1.7 **Kryptographische Basisdienste**	7.1.8 **TLS-Kanäle unter Nutzung sicherer kryptographischer**
FCS_CKM.1/NK							X	
FCS_CKM.2/NK.IKE							X	
FCS_CKM.4/NK							X	X
FTP_ITC.1/NK.TLS						X		X
FPT_TDC.1/NK.TLS.Zert								X
FCS_CKM.1/NK.TLS								X
FCS_COP.1/NK.TLS.HMAC								X
FCS_COP.1/NK.TLS.AES								X
FCS_COP.1/NK.TLS.Auth								X
FCS_CKM.1/NK.Zert								X
FDP_ETC.2/NK.TLS								X
FDP_ITC.2/NK.TLS								X
FDP_ETC.2/NK.TLS								X
FMT_MOF.1/NK.TLS								X
FDP_ACC.1/NK.Update						X		
FDP_ACF.1/NK.Update						X		
FTP_ITC.1/NK.KSR						X		
FDP_UIT.1/NK.Update						X		

Tabelle 11: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen

7.2.2. Erfüllung der funktionalen Sicherheitsanforderungen

Wie aus der Tabelle 11 ersichtlich, wird jede Sicherheitsanforderung gemäß Kapitel 6.2 durch die Sicherheitsfunktionen in Kapitel 7.1 umgesetzt. Die Beschreibung der Sicherheitsfunktionen in den Kapiteln 7.1.1-7.1.8 nutzen direkte Referenzen auf die entsprechenden implementierten Sicherheitsfunktionen in Kapiteln 6.2.1-6.2.8. Die Sicherheitsfunktionen sind dabei direkt aus der Unterteilung der Sicherheitsfunktionen im -PP [11] abgeleitet.

8. Anhang

8.1. Gesetzliche Anforderungen

Das fünfte Sozialgesetzbuch [9] fordert in § 291a „Elektronische Gesundheitskarte“ die Erweiterung der Krankenversichertenkarte zu einer elektronischen Gesundheitskarte und definiert darin die Pflichtanwendungen

- Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form (sogenannte elektronische Verordnung oder „eVerordnung“) und

- Berechtigungsnachweis zur Inanspruchnahme von medizinischen Leistungen (dies umfasst – wie schon bisher durch die Krankenversichertenkarte – die Abfrage von Versichertenstammdaten und Zuzahlungsstatus).

Ferner definiert das Gesetz die folgenden freiwilligen Anwendungen, bei denen dem Versicherten die Teilnahme freigestellt wird:

- Speicherung von medizinischen Notfalldaten (beispielsweise zum Abruf dieser Daten durch den Notarzt an einem Unfallort),

- elektronischer Arztbrief (auf diese Weise sollen Ärzte im Falle einer Überweisung eines Versicherten Befunde, Diagnose, Therapieempfehlungen sowie Behandlungsberichte austauschen können),

- Speicherung von Daten zur Prüfung der Arzneimitteltherapiesicherheit (das Ziel ist hier die frühzeitige Erkennung von Arzneimittelunverträglichkeiten) und

- Speicherung von Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (sogenannte „elektronische Patientenakte“),

- Speicherung von durch die Versicherten selbst oder für sie zur Verfügung gestellten Daten, sowie

- Speicherung von Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten.

Im Rahmen der genannten freiwilligen Anwendungen werden Daten erhoben, gespeichert, verarbeitet und genutzt.

Der Konnektor unterstützt sowohl Pflichtanwendungen als auch freiwillige Anwendungen. Anforderungen an den Konnektor wurden bisher nur aus den Pflichtanwendungen abgeleitet.

Anwendungshinweis 109: Der Anwendungskonnektor ist dafür verantwortlich, dass medizinische Daten, die vom EVG verarbeitet werden, bereits verschlüsselt sind, wenn sie an den EVG übergeben werden.

8.2. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AH	Authentication Header, siehe RFC 2402 und RFC 4302 [28]
AK	Anwendungskonnektor: Der Teil des Gesamtkonnektors, der nicht Netzkonnektor ist, wird als Anwendungskonnektor bezeichnet.
AK-PP	Schutzprofil (Protection Profile) für den Anwendungskonnektor
AVS	Apothekenverwaltungssystem
BA	Berufsausweis
Bestands-netz	Bestehende Netzwerke oder zukünftige sektorale Netze, die Anschluss an die TI erhalten sollen.
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (siehe www.bundesnetzagentur.de)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CAMS	Card Application Management System
CRL, CRLs	Certificate Revocation List(s)
CS	Clientsystem
DHCP	Dynamic Host Configuration Protocol: Protokoll, das die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server realisiert
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information (siehe www.dimdi.de) , eine nachgeordnete Behörde des Bundesministeriums für Gesundheit (BMG)
DoS	Denial of Service, übersetzt etwa Dienstverweigerung; bezeichnet einen Angriff auf einen Server mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen; in der Regel geschieht dies durch Überlastung
DRNG	Deterministic Random Number Generator deterministischer Zufallszahlengenerator (siehe [5])
DSL	Digital Subscriber Line
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card (englischer Begriff für eGK)
ESP	Encapsulating Security Payload; siehe RFC 2406 [29] bzw. zukünftig RFC 4303 [30]; für die jeweils zu verwendenden Standards siehe die Konnektorspezifikation [16]
gematik	gematik GmbH, siehe https://www.gematik.de
GKV	gesetzliche Krankenversicherung
HBA	Heilberufsausweis

Abkürzung	Bedeutung
HPC	Health Professional Card (englischer Begriff für HBA)
HSM	High Security Modul, Hochsicherheitsmodul; sicherer Schlüsselspeicher mit der Möglichkeit, kryptographische Berechnungen auszuführen, ohne dass das Schlüsselmaterial das HSM verlässt
HSM-B	Eine HSM-Variante einer Institutionskarte Typ B (Secure Module Card). Das SM-B wird in dieser Fassung als virtuelle Karte verstanden, welches in einem virtuellen Kartenterminal steckt.
IAG	Internetzugangspunkt des Leistungserbringers
IKE	Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 [31]
IP	Internet Protocol
IPsec	IP Security, vgl. RFC 2401 bzw. RFC 4301 [27]
IPv4	Internet Protocol version 4, siehe RFC 791
IPv6	Internet Protocol version 6, siehe RFC 2460
KIS	Krankenhausinformationssystem
LE	Leistungserbringer
KV	Kassenärztliche Vereinigung
LAN	lokales Netzwerk (local area network), meist im Zusammenhang mit dem lokalen Netzwerk eines Leistungserbringers verwendet
LS*n*	logische Schnittstelle Nr. *n* (siehe Abschnitt 1.3.3.2)
MAC	Message Authentication Code; kryptographische Prüfsumme zum Schutz der Datenintegrität; vergleichbar einer Signatur, aber erstellt unter Verwendung eines symmetrischen Kryptoalgorithmus’
NAT	Network Address Translation, siehe RFC 2663
NK	Netzkonnektor, einer der Hauptfunktionsblöcke des Konnektors (siehe auch AK)
NTP	Network Time Protocol, siehe RFC 958 (Sept. 1985) und NTP Version 4 Release Notes (Okt. 2005)
OCSP	Online Certificate Status Protocol, siehe RFC 2560
PIN	Persönliche Identifikationsnummer, dient zur Authentisierung eines menschlichen Benutzers gegenüber einem IT-System (hier: gSMC-K)
PKV	private Krankenversicherung
PP	Protection Profile (Schutzprofil)
PS*n*	physische Schnittstelle Nr. *n* (siehe Abschnitt 1.3.3.1)
PVS	Praxisverwaltungssystem
RFC	Request for comment, siehe http://tools.ietf.org/html/

Abkürzung	Bedeutung
RSA	asymmetrisches Kryptoverfahren, benannt nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman
SAK	Bezeichnung einer Identität des Konnektors; steht für Signaturanwendungskomponente (einem Begriff aus dem Signaturgesetz)
SAR	Security Assurance Requirement Anforderung an die Vertrauenswürdigkeit des EVG
SFR	Security Functional Requirement funktionale Sicherheitsanforderung an den EVG
SGB V	Sozialgesetzbuch, fünftes Buch; dessen § 291a beschreibt die Einführung der elektronischen Gesundheitskarte
SICCT	Secure Interoperable Chip Card Terminal, Kartenleser
SIS	Sicherer Internet Service: Ein Internet-Zugangspunkt, der die damit verbundenen lokalen Netze und Systeme gegen Angriffe aus dem Internet schützt.
SM-B	Zusammenfassender Begriff für eine SMC-B (Institutionskarte Typ B), als auch eine in einem HSM-B (Hardware Security Module) enthaltene virtuelle SMC-B.
SMC	Security Module Card, Sicherheitsmodul (hier: Chipkarte als sicherer Schlüsselspeicher)
SMC-B	Security Module Card, Typ B, Träger der kryptographischen Identität der Institution des Leistungserbringers; wird u. a. vom AK zur Authentisierung gegenüber zentralen Diensten (Fachanwendungen) verwendet
gSMC-K	Geräte-Security Module Card Konnkektor: Sicherheitsmodul (für den) Netzkonnektor Bezeichnung für die Anwendung auf dem Sicherheitsmodul SM-K (oder einem der Sicherheitsmodule SM-K) des Einbox-Konnektors, welches das vom NK benötigte Schlüsselmaterial speichert. Träger der kryptographischen Identität des Netzkonnektors; wird insbesondere vom Netzkonnektor zur Authentisierung gegenüber dem VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform verwendet.
SM-K	Sicherheitsmodel für den Konnektor, kann z. B. in Form einer Chipkarte ausgeprägt sein; falls das SM-K die *Spezifikation der gSMC-K* / Objektsystem [20] erfüllt, wird es als SMC-K bezeichnet
SM-KT	Sicherheitsmodul für das Kartenterminal
SM-SAK	Sicherheitsmodul (für die) Signaturanwendungskomponente (SAK) des Konnektors

Abkürzung	Bedeutung
	Bezeichnung für die Anwendung auf dem Sicherheitsmodul SM-K (oder einem der Sicherheitsmodule SM-K) des Einbox-Konnektors, welches das von der Signaturanwendung benötigte Schlüsselmaterial speichert.
SNTP	Simple Network Time Protocol, siehe RFC 4330
SSCD	Secure Signature Creation Device, englisches Pendant zu SSEE
SSEE	Sichere Signaturerstellungseinheit, deutsches Pendant zu SSCD
SSL	Secure Sockets Layer, Kommunikationsprotokoll ersetzt durch TLS.
ST	Security Target
ST-Autor	Autor des Security Targets (welches basierend auf diesem PP erstellt wird)
TCP	Transmission Control Protocol, siehe RFC 793 und RFC 1323
TLS	Transport Layer Security
EVG	Target of evaluation; (deutsches Synonym: Evaluationsgegenstand, abgekürzt: EVG)
TSF	EVG Security Functionality (Definition aus CC v3.1 R5, Teil 1 [1]: „combined functionality of all hardware, software, and firmware of a EVG that must be relied upon for the correct enforcement of the SFRs”
TSL	Trust-Service Status List, siehe Glossar, Kapitel 8.3
USB	Universal Serial Bus
VODD	Verordnungsdaten-Dienst; zentraler Dienst zur Verwaltung von Verordnungen (umgangssprachlich: „Rezepten“)
VPN	virtuelles (nur logisch getrennt existierendes) privates Netz (virtual private network) Ein VPN nutzt ein offenes, ungeschütztes Netz (z. B. das Internet) als Transportmedium und ermöglicht darauf eine gesicherte Verbindung zwischen den rechtmäßigen Teilnehmern des VPNs, die sich durch den Besitz kryptographischer Schlüssel als solche ausweisen. Die in einem VPN übertragenen Daten werden in aller Regel durch Verschlüsselung gegen unbefugte Kenntnisnahme und durch kryptographische Prüfsummen gegen unbemerkte Veränderung geschützt.
VPN-TI	VPN-Konzentrator für den Zugriff auf die zentrale Telematikinfrastruktur-Plattform
VPN-SIS	VPN-Konzentrator für den Zugriff auf den Internet-Zugangspunkt (SIS)
VSD	Versicherten-Stammdaten
VSDD	Versicherten-Stammdaten-Dienst (zentraler Dienst)
WAN	Weitverkehrsnetzwerk (wide area network), meist im für das Transportnetz zur Anbindung der Leistungserbringer an die zentrale Telematikinfrastruktur-

Abkürzung	Bedeutung
	Plattform verwendet; beispielsweise kann das Internet als Transportmedium für ein VPN genutzt werden
X.509	Standard der ITU-T (International Telecommunication Union) für Public Key Infrastrukturen und insbesondere für den Aufbau von Zertifikaten

Tabelle 12: Abkürzungsverzeichnis

8.3. Glossar

Begriff	Bedeutung
application connector	Anwendungskonnektor
Attacker	Angreifer (siehe auch Abschnitt 3.2)
Bestandsnetze	Bestehende Netzwerke, die (zukünftig) Anschluss an die TI erhalten sollen.
Box	Der Begriff Box wird im Zusammenhang mit den Begriffen „Einbox-Konnektor“ bzw. „Einboxlösung“ und „Mehrkomponentenlösung“ bzw. „Mehrkomponenten-Konnektor“ verwendet. Die „Box“ bezeichnet dabei ein gemeinsames Gehäuse. Wenn eine Einboxlösung in sicherer Umgebung steht (was sie gemäß der Annahme A.phys_Schutz tut), dann kann es keine Angriffe auf die interne Kommunikation zwischen den Konnektorteilen (NK, AK, gSMC-K) geben. Im Fall einer Mehrboxlösung werden Angriffe auf die Kommunikation zwischen den Konnektorteilen betrachtet. Diese Angriffe müssen dann entweder technisch (z. B. durch gegenseitige Authentisierung und den Aufbau eines sicheren Kanals) oder organisatorisch abgewehrt werden.
sicherer Schlüsselspeicher	Bezeichnung für die Fähigkeit des EVGs, Schlüsselmaterial vor unbefugter Kenntnisnahme und Verfälschung geschützt sicher speichern zu können.
stateful packet inspection, stateful inspection	dynamische Paketfiltertechnik, bei der (sofern es die Systemressourcen zulassen; im Fall eines denial-of-service-Angriffs müssen Datenpakete verworfen werden) jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird; der Verbindungsstatus eines Datenpakets wird in die Entscheidung einbezogen, ob ein Informationsfluss zulässig ist oder nicht
Transportnetz	Netz, welches als Transportmedium für die Datenübermittlung genutzt wird; in sehr häufigen Fällen das Internet, über welches durch VPN-Tunnel geschützt Daten zwischen dezentralen Standorten der Leistungserbringer und Rechenzentren der zentralen Telematikinfrastruktur-Plattform übertragen werden

Begriff	Bedeutung
Trust-Service Status List (TSL)	Eine Trust-service Status List bietet alle relevanten Informationen zur vertrauenswürdigen Verteilung und Prüfung der Wurzelzertifikate verschiedener „Certification Authorities“ in Form einer signierten XML-Datei (ETSI-Standard). Hierdurch können auch bereits existierende heterogene PKI´s nach einem einheitlichen Schema eingebunden werden.
VPN concentrator	VPN-Konzentrator
VPN-Konzentrator für den Zugang zur Telematikinfrastruktur	VPN-Konzentrator, welcher einen Zugang zur Telematikinfrastruktur bereitstellt – und damit auch einen Zugang für Dienste gemäß § 291 a SGB V (Pflichtanwendungen und freiwillige Anwendungen)
workstation	Im Schutzprofil gewählte englische Übersetzung für den deutschen Begriff Clientsystem bzw. Arbeitsplatz des Clientsystems zur Formulierung der SFRs.
Zugangsnetz zur Telematikinfrastruktur	Plattform zur Anbindung der Leistungserbringer an die zentrale Telematikinfrastruktur-Plattform. „*Das Zugangsnetz zur Telematikinfrastruktur ermöglicht es Leistungserbringern, mit den zugeordneten Infrastrukturdiensten und Brokern kontrolliert und sicher zu kommunizieren. So können medizinische Datenobjekte zwischen den Leistungserbringern und den Fachdiensten sicher transportiert werden. Das Zugangsnetz ist der äußere Teil des abgeschlossenen und gesicherten Telematiknetzes.* *Der Leistungserbringer muss mit zertifizierten und zugelassenen Komponenten ausgestattet sein (SM-K und Konnektor), die die Telematiksicherheitsrichtlinien erfüllen. Ohne diese spezielle Infrastruktur beim Leistungserbringer ist es nicht möglich, einen Kommunikationskanal in die Telematikinfrastruktur aufzubauen.* […]“

Tabelle 13: Glossar[167]

8.4. Abbildungsverzeichnis

[167] Weitere Abkürzungen s. BSI-CC-PP-0097-V2-2020-MA-02, Abschnitt 7.3.

8.5. Tabellenverzeichnis

8.6. Literaturverzeichnis

8.6.1. Kriterien

[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

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

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

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

[6] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[7] Joint Interprtation Library, Composite evaluation of Smart Cards and similar devices, January 2012, Version 1.2

[8] W. Killmann, W. Schindler: A proposal for: Functionality classes for random number generators. Version 2.0, September 2011

8.6.2. Gesetze und Verordnungen

[9] Fünftes Buch Sozialgesetzbuch (SGB V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477), zuletzt geändert durch Artikel 6 des Gesetzes vom 28. Mai 2008 (BGBl. I S. 874)

8.6.3. Schutzprofile (Protection Profiles) und Technische Richtlinien

[10] Common Criteria Protection Profile: Card Operating System (PP COS), BSI-CC-PP-0082- 2013, 06.09.2013 und jede darauf angewandte Maintenance und Rezertifizierung, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097-V2-2020-MA-02, Version 1.6.7 vom 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Common Criteria Protection, Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-03, Version 1.6.2 vom 21.08.2024, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] Technische Richtlinie TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Bundesamt für Sicherheit in der Informationstechnik, Version 2019-01

[14] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Bundesamt für Sicherheit in der Informationstechnik, Version 3.20, 21.09.2018, Technische Arbeitsgruppe TR-03116-1

[14a] Technische Richtlinie BSI TR-03111 Elliptic Curve Cryptography, Version 2.10, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] Technische Richtlinie BSI TR-03144, eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Bundesamt für Sicherheit in der Informationstechnik, Version 1.2, 27.07.2017

8.6.4. Spezifikationen

[16] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon], Version 5.24.0, 26.07.2024, gematik GmbH

[17] Elektronische Gesundheitskarte und Telematikinfrastruktur: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik GmbH, Version 1.28.1, 09.08.2024

[18] Elektronische Gesundheitskarte und Telematikinfrastruktur: Übergreifende Spezifikation. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik GmbH, Version 2.35.0, 05.07.2024

[19] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation des Card Operating System (COS) Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik GmbH

[20] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation der gSMC-K / Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.14.0, 12.05.2022, gematik GmbH

[21] UEFI, Unified Extensible Firmware Interface Specification, Version 2.7, May 2017, Unified EFI Forum

8.6.5. Standards

[22] D. Mills, U.Delaware, J. Martin, J.Burbank, W.Kasch: Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010, RFC 5905 (NTPv4), https://www.ietf.org/rfc/rfc5905.txt

[23] 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

[23a] M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. March 2010, RFC 5639, https://www.rfc-editor.org/rfc/rfc5639.txt

[24] 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

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

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

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

[28] S. Kent: IP Authentication Header, December 2005, RFC 4302 (AH), https://www.ietf.org/rfc/rfc4302.txt

[29] S. Kent, R. Atkinson: IP Encapsulating Security Payload (ESP), November 1998, RFC 2406 (ESP), https://www.ietf.org/rfc/rfc2406.txt

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

[31] 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/rfc5996.txt

[32] T. Kivinen, B. Swander, A. Huttunen, V. Volpe: Negotiation of NAT-Traversal in the IKE, January 2005, RFC 3947 (NAT-Traversal in IKE) https://www.ietf.org/rfc/rfc7296.txt

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

[34] 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

[35] 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

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

[37] R. Droms: Dynamic Host Configuration Protocol. March 1997, RFC 2131, https://www.ietf.org/rfc/rfc2131.txt

[38] S. Alexandwer, R. Droms: DHCP Options and BOOTP Vendor Extensions. March 1997, RFC 2132, https://www.ietf.org/rfc/rfc2132.txt

[39] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose: Protocol Modifications for the DNS Security Extensions. March 2005, RFC 4035, https://www.ietf.org/rfc/rfc4035.txt

[40] RFC 8446 (August 2018): The Transport Layer Security (TLS) Protocol, Version 1.3

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

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

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

[44] RFC 8422 (August 2018) Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), Versions 1.2 and earlier

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

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

[47] 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), http://www.ietf.org/rfc/rfc5280.txt

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

[49] W. Polk, R. Housley, L. Bassham: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3279 (April 2001), http://www.ietf.org/rfc/rfc3279.txt

[50] M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639 (March 2010), http://www.ietf.org/rfc/rfc5639.txt

[51] RFC 7027: (October 2013) Elliptic Curve Cryptography (ECC) Brainpool, Curves for Transport Layer Security (TLS), https://tools.ietf.org/html/rfc7027

8.6.6. Bedienhandbuch

Die gültigen Versionen der Dokumente in diesem Abschnitt sind dem Zertifizierungsreport zu entnehmen, der zusammen mit diesen Sicherheitsvorgaben von der Zertifzierungsstelle veröffentlicht wird.

[52] RISE Konnektor Bedienungsanleitung [RISE-KON-AGD_OPE]