Security Target für secunet konnektor 2.0.0 und secunet konnektor 2.1.0
Einbox-Konnektor und Rechenzentrums-Konnektor

secunet Security Networks AG
Kurfürstenstraße 58,
45138 Essen
Internet: www.secunet.com

Änderungsverlauf

Version	Datum	Änderungen	Anmerkungen
1.0	10.03.2023	Initiale Version	Initiale Version basierend auf dem PTV5 WR1 ST (BSI-DSZ-CC-1044-V6-2022), Version 1.2 vom 25.10.2022
1.1	26.06.2023	Neue PP Version, Formale Anpassungen	-
1.2	21.08.2023	Anpassungen zur Laufzeitverlängerung	-
1.3	21.08.2023	Kommentare der Prüfstelle	-
1.4	24.08.2023	Anpassungen der Version des TOE	
1.5	06.10.2023	Anpassungen der Version des TOE	
1.6	21.03.2024	Anpassungen der Version des TOE	
1.7	07.08.2024	Deterministischen RNG ergänzt	
1.8	15.08.2024	Anpassungen der Version des TOE	
1.9	26.09.2024	Anpassungen der Version des TOE	
2.0	11.11.2024	RZK und EBK STs zusammgengeführt	
2.1	18.12.2024	Kommentare der Prüfstelle umgesetzt	
2.2	14.01.2025	Kommentare der Prüfstelle umgesetzt	
2.3	24.01.2025	Kommentare der Prüfstelle umgesetzt	
2.4	08.04.2025	Referenz auf Handbuch korrigiert	
2.5	10.04.2025	Referenz auf Handbuch korrigiert	

Inhaltsverzeichnis

1. ST-Einführung 7

1.1. ST-Referenz 7

1.2. ST-Übersicht 9
1.2.1. TOE Konfigurationen 9
1.2.2. Abgrenzung 9
1.2.3. Terminologie 10

1.3. EVG-Beschreibung 11
1.3.1. EVG-Typ 11
1.3.2. Einsatzumgebung des Konnektors 14
1.3.3. Schnittstellen des Konnektors 17
1.3.4. Aufbau und physische Abgrenzung des Netzkonnektors 20
1.3.5. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste 23
1.3.6. Non-EVG hardware/software/firmware 26

2. Postulat der Übereinstimmung 28

2.1. Common Criteria Konformität 28

2.2. Security Target-Konformität 28

2.3. Paket-Konformität 28

2.4. Begründung der Konformität 28

2.5. ST-Organisation 29

3. Definition des Sicherheitsproblems 30

3.1. Zu schützende Werte 30
3.1.1. Primäre Werte 30
3.1.2. Sekundäre Werte 33

3.2. Externe Einheiten, Subjekte und Objekte 35
3.2.1. Externe Einheiten (*external entities*) 35
3.2.2. Objekte 36

3.3. Bedrohungen 37
3.3.1. Auswahl der betrachteten Bedrohungen 37
3.3.2. Liste der Bedrohungen 37

3.4. Organisatorische Sicherheitspolitiken 44

3.5. Annahmen 45

4. Sicherheitsziele 50

4.1. Sicherheitsziele für den EVG 50
4.1.1. Allgemeine Ziele: Schutz und Administration 50
4.1.2. Ziele für die VPN-Funktionalität 53
4.1.3. Ziele für die Paketfilter-Funktionalität 54

4.2. Sicherheitsziele für die Umgebung 55

4.3. Erklärung der Sicherheitsziele (Security Objectives Rationale).....63
4.3.1. Überblick: Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele 63
4.3.2. Abwehr der Bedrohungen durch die Sicherheitsziele 64
4.3.3. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele 70
4.3.4. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung.....71

5. Definition zusätzlicher Komponenten.....72

5.1. Definition der erweiterten Familie FPT_EMS und der Anforderung FPT_EMS.1.....72

6. Sicherheitsanforderungen 73
6.1.1. Hinweise zur Notation.....73

6.2. Funktionale EVG-Sicherheitsanforderungen.....73
6.2.1. VPN-Client 74
6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung 76
6.2.3. Netzdienste.....87
6.2.4. Stateful Packet Inspection.....89
6.2.5. Selbstschutz.....89
6.2.6. Administration 94
6.2.7. Kryptographische Basisdienste 102
6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen 107

6.3. Anforderungen an die Vertrauenswürdigkeit des EVG.....118
6.3.1. Verfeinerung von ALC_DEL.1.....118
6.3.2. Verfeinerungen von AGD_OPE.1.....118
6.3.3. Verfeinerung von ADV_ARC 119

6.4. Erklärung der Sicherheitsanforderungen (Security Requirements Rationale).....121
6.4.1. Abbildung der EVG-Ziele auf Sicherheitsanforderungen 121
6.4.2. Erfüllung der Abhängigkeiten.....133

6.5. Erklärung für Erweiterungen 134

6.6. Erklärung für die gewählte EAL-Stufe.....134

7. Zusammenfassung der EVG Sicherheitsfunktionalität.....135

7.1. Sicherheitsfunktionen des EVG 135
7.1.1. VPN-Client 135
7.1.2. Dynamischer Paketfilter 136
7.1.3. Netzdienste.....136
7.1.4. Stateful Packet Inspection.....137
7.1.5. Selbstschutz.....137
7.1.6. Administration 138
7.1.7. Kryptographische Basisdienste 139
7.1.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen 140

7.2. Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen 141
7.2.1. Überblick 141
7.2.2. Erfüllung der funktionalen Sicherheitsanforderungen 142
8. Anhang 143
8.1. Gesetzliche Anforderungen 143
8.2. Abkürzungsverzeichnis 144
8.3. Glossar 148
8.4. Abbildungsverzeichnis 150
8.5. Tabellenverzeichnis 150
8.6. Literaturverzeichnis 151
8.6.1. Kriterien 151
8.6.2. Gesetze und Verordnungen 151
8.6.3. Schutzprofile und Technische Richtlinien 151
8.6.4. Spezifikationen 152
8.6.5. Standards 153
8.6.6. Dokumentation 154

1. ST-Einführung

1.1. ST-Referenz

Titel:	Security Target für secunet konnektor 2.0.0 und secunet konnektor 2.1.0
Version des Dokuments:	2.5
Datum des Dokuments:	10.04.2025
Allgemeiner Status:	ST zur Evaluierung
ST-Registrierung:	BSI-DSZ-CC-1044-V8-2024
NK-PP Registrierung:	BSI-CC-PP-0097
NK-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:	secunet AG
TOE Name.	secunet konnektor 2.0.0 und secunet konnektor 2.1.0
TOE Version	5.70.4:2.0.0 und 5.70.4:2.1.0
Stichwörter:	Konnektor, Netzkonnektor, eHealth, elektronisches Gesundheitswesen, Telematikinfrastruktur, dezentrale Komponente, secunet konnektor

Dieses Security Target wurde konform zu den folgenden Dokumenten

[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

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

erstellt. Darüber hinaus orientiert sich dieses Dokument in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang in Abschnitt 8.6 (insbesondere Abschnitt 8.6.4) aufgeführt sind; allen voran die Konnektorspezifikation:

[17] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon]: Version 5.20.0, 05.05.2023, gematik GmbH,

1.2. ST-Übersicht

Dieses Security Target beschreibt den Schutzbedarf für den Netzkonnektor secunet konnektor 2.0.0 sowie secunet konnektor 2.1.0 als Bestandteil des Konnektors im Gesundheitswesen gemäß Spezifikation [17]. Im Folgenden wird zu Vereinfachung oft nur der Konnektor in Hardware Version 2.0.0 aufgeführt. Das ST bezieht sich aber auf beide Hardware-Konfigurationen (2.0.0 und 2.1.0). Zu den gesetzlichen Grundlagen siehe Abschnitt 8.1 *Gesetzliche Anforderungen* im Anhang. Der Konnektor ist darauf ausgerichtet, durch Weiterentwicklung und Update im Feld für weitere Versionen nachgenutzt zu werden.

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. TOE Konfigurationen

Dieses Security Target beschreibt zwei Konfigurationen des secunet konnektor: den secunet konnektor 2.0.0 und den secunet konnektor 2.1.0.

Bei der Basiskonfiguration (dem secunet konnektor 2.0.0) handelt es sich um einen Konnektor (auch als Einboxkonnektor oder EBK bezeichnet).

Bei der als Rechenzentrums-Konnektor bezeichneten Variante (auch RZK oder secunet konnektor 2.1.0) handelt es sich um eine typische Lösung für kleinere und mittlere ArztpraxenRechenzentren in Krankenhäusern oder Apothekenandere Einrichtungen: Netzkonnektor und Anwendungskonnektor laufen in einer gemeinsamen Box ab. Es handelt sich also um zwei Einbox-Konnektoren, die (ohne Einbox-Gehäuse) in einem 19 Zoll Gehäuse mit einer Höheneinheit verbaut sind.

1.2.2. Abgrenzung

Das Schutzprofil BSI-CC-PP-0098 [11] 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 schließt die gSMC-K als Teil der IT-Umgebung ein. Die relevanten Sicherheitsziele der Einsatzumgebung, wie OE.NK.gSMC-K, OE.NK.KeyStorage und OE.NK.RNG beziehen sich auf die Funktionalität der gSMC-K.

Die Konnektorspezifikation [17] 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 [11] mit den Sicherheitsanforderungen an den Konnektor (ohne gSMC-K) verwiesen.

1.2.3. Terminologie

Der „Evaluierungsgegenstand“ (EVG, englisch „Target of Evaluation“, TOE) der durch dieses Security Target definiert wird, wird als Netzkonnetor bezeichnet.

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] 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, http://www.bmg.bund.de), der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik, http://www.gematik.de) und des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI, http://www.dimdi.de) verwiesen. Das Projekt-Glossar der gematik wird unter gemSpec_Kon [17] 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

1.3. EVG-Beschreibung

Der Evaluierungsgegenstand ist:

- der Netzkonnektor, secunet konnektor 2.0.0 als Teil des Konnektors für den Online-Rollout (Stufe 1) welcher als eine **Einbox-Lösung** implementiert wird.

Der EVG secunet konnektor 2.0.0 umfasst die Software des Netzkonnektors und die dazugehörige Dokumentation für Administratoren und Benutzer [52], [53] und [54].

Komponenten des Konnektors	**Version**
Hardware (nicht Teil des EVG)	2.0.0 und 2.1.0
BIOS FW für Hardware Version 2.0.0 (nicht Teil des EVG)	CSASR009 oder CSASR011
BIOS FW für Hardware Version 2.1.0 (nicht Teil des EVG)	CSASR011
Softwareversion Netzkonnektor[3]	5.70.4
Softwareversion Anwendungskonnektor	5.70.3
Bedienhandbuch	6.8.5
Hinweise und Prüfpunkte für Endnutzer	2.0
REST-API Spezifikation	5.1.1

Tabelle 1: Komponenten der Einbox-Lösung

1.3.1. EVG-Typ

Der Konnektor stellt einen neuen Produkttyp dar, so dass außer dem Gattungsbegriff „Konnektor“ kein weiterer TOE 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] Mit dieser Versionsnummer ist auch die Version des Anwendungskonnektors fest bestimmt. Zur exakten bestimmung der TOE version reicht daher die Angabe der Softwareversion des Netzkonnektor.

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

Die Sicherheitsfunktionalität

- einer Firewall,
- eines VPN-Clients,
- von Servern für Zeitdienst, Namensdienst und DHCP-Dienst, und
- die Basisdienste zum Aufbau von TLS-Kanälen,

werden durch den Bestandteil Netzkonnektor (**EVG**, secunet konnektor 2.0.0) erbracht.

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 (**nicht Teil der Evaluierung**).

Das Sicherheitsmodul gSMC-K stellt interne Sicherheitsfunktionalität zur Speicherung von Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit (**nicht Teil der Evaluierung**).

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

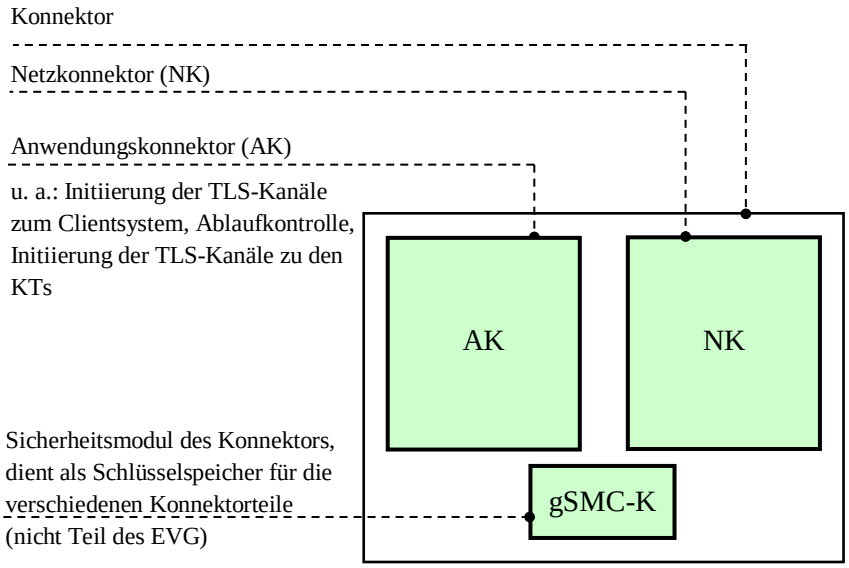

Abbildung 1: Funktionsblöcke des Konnektors

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.

Anwendungshinweis 1: Siehe Kapitel 1.3.1 des PP [12]

Anwendungshinweis 2: Kapitel 1.3.1 des PP [12].

1.3.2. Einsatzumgebung des Konnektors

Die Einsatzumgebung des Konnektors als Einbox-Lösung ist in der folgenden Abbildung 2 dargestellt. Insbesondere wird der Netzkonnektor immer mit Konnektorteilen (AK und gSMC-K) gemeinsam betrieben, die nach den für diese Konnektorteile anzuwendenden Schutzprofilen 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. Der physische Zugriff auf die benannten Schnittstellen ist durch **A.NK.phys_Schutz** ausgeschlossen. Der logische Schutz der Schnittstellen ist Teil der Sicherheitsfunktionalität, die Gegenstand des EVG ist.

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

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

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 (EVG) als ein Teil des Konnektors ist durch dunkelblaue Färbung kenntlich gemacht. Die Übrigen Teile des Konnektors sind hellblau dargestellt. Durch die dunkelblaue Färbung wird die physische EVG-Abgrenzung des Netzkonnektors beschrieben. Mit der roten Linie werden zum besseren Verständnis Komponenten zusammengefasst, die in einem gemeinsamen Gehäuse untergebracht sind oder die üblicherweise auf einer gemeinsamen Plattform ablaufen. Die roten Linien beschreibt den physikalisch geschützten Bereich (vgl. A.NK.phys_Schutz).

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

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

- NK: Netzkonnektor (EVG)
- AK: Anwendungskonnektor
- 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: Im Konnektorgehäuse ist physisch kein WAN-Router integriert.

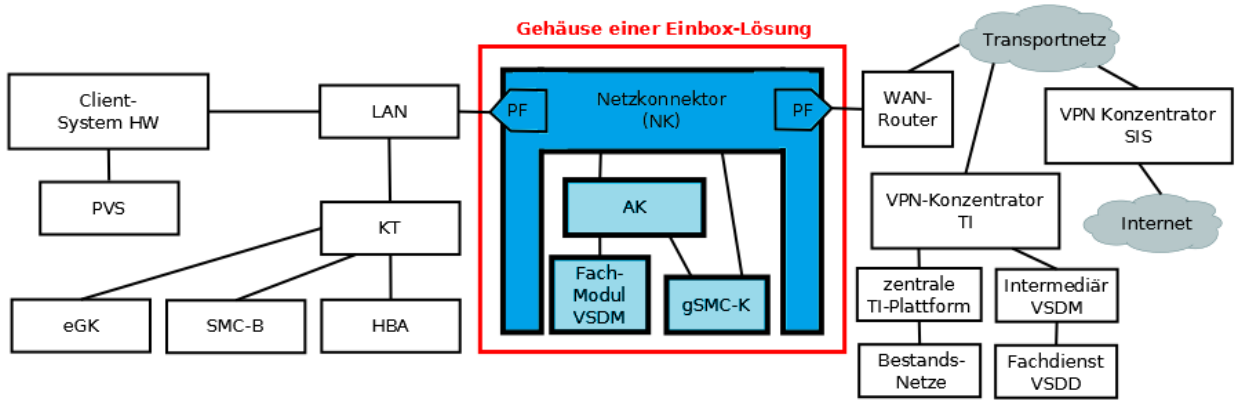

Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung)

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.

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: Nicht relevant.

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: **Spezielle Annahmen:** Außer den benannten Annahmen an die sichere Infrasturktur und Implementierung der Clientsysteme werden keine weiteren Annahmen getroffen.

Anwendungshinweis 8: **Spezielle Einsatzumgebungen:** Für den EVG als Teil des Produkts sind keine zusätzlichen Einsatzszenarien die über das zugrundeliegende PP [12] hinausgegehen geplant. Es ergeben sich keine zusätzlichen Anforderungen an die Umgebung.

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 9: Der EVG unterstützt alle vom NK-PP [12] erwarteten physischen Schnittstellen und implementiert darüber hinaus herstellerspezifische Schnittstellen wie im Folgenden dargestellt.

Der EVG besitzt folgende physische Schnittstellen:

PS1 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 SIS dienen. Es wird angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und Verbindungen mit ihnen nicht notwendigerweise verschlüsselt sind. Da der EVG zwei Netzwerkkarten nutzt, findet eine physische Trennung des LAN- bzw. WAN-Zugangs über die Netzwerkkarten statt. Die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle fallen nicht in einer physischen Schnittstelle zusammen.

Anwendungshinweis 10: Durch die für dieses ST relevante Einboxlösung des Konnektors ist die Identifizierung einer physischen Schnittstelle zwischen Netzkonnektor und dem Anwendungskonnektor nicht relevant. Die Kommunikation beider Konnektorteile beschränkt sich auf die logische Schnittstelle LS1. In diesem ST wird die Nummerierung aus dem NK-PP [12] beibehalten. Die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle sind durch separate Netzwerkcontroller physisch getrennt.

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 Schnittstelle zu einer Signaleinrichtung mit Status LEDs

Der EVG verfügt über eine Schnittstelle zu einer Signaleinrichtung mit sieben Status-LEDs zur Anzeige des aktuellen Betriebszustands des Konnektors. Die LEDs sind wie folgt belegt: Power On, Betriebszustand, 2x VPN Verbindungszustand (VPN TI, VPN SIS), Fehlerzustand, Remote Administration, Update verfügbar

PS6 Eine USB Schnittstelle.

Die USB2.0 Schnittstelle wird für die initialisierung des EVG im Rahmen der TOE Entwicklung verwendet. Im Operativen Betrieb wird diese Schnittstelle nicht verwendet. Es wird angenommen, dass der Zugriff auf diese Schnitstelle auf eine sichere Weise erfolgt (siehe A.NK.phys**_Schutz** sowie A.NK.Admin_EVG).

PS7 Eine Schnittstelle für den Werksreset.

Am Gehäuse ist ein gegen unbeabsichtigte Auslösung gesicherten Reset-Taster angebracht, mit dem ein Werksreset des EVGs ausgelöst werden kann.

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. Die 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 [12].

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

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 NK-PP [12] sind enthalten. Es sind zusätzliche Schnittstellen definiert worden.

Der EVG besitzt folgende logische Schnittstellen:

LS1 Eine Schnittstelle zum Anwendungskonnektor. Über diese Schnittstelle werden auch die Managementfunktionen zur Administrierung des Netzkonnektors durch den Anwendungskonnektor aufgerufen.

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

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

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

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

LS6 Eine Schnittstelle zu lokalen Managementfunktionen (Software/Firmware, TSL-Updates, Firewall-Konfiguration) des Netzkonnektors (via PS2).

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

LS8 Eine Schnittstelle zu entfernten Managementfunktionen für den Netzkonnektor gemäß Konnektor-Spezifikation [17], Abschnitt 4.3.8 (via PS2).

LS9 Eine Schnittstelle zur Signaleinrichtung zur Anzeige von Hinweisen an den Administrator über kritische Betriebszustände des Konnektors gemäß Konnektor-Spezifikation [17], Abschnitt 3.3 (via PS5).

LS10 Eine USB-Schnittstelle zur initialisierung des EVG. Im Operativen Betrieb wird diese Schnittstelle nicht verwendet und daher nicht weiter betrachtetInsbesondere werden keine Bedrohungen in Bezug auf diese Schnittstelle betrachtet, da die Schnittstelle aufgrund der Annahmen an die Zugänglichkeit als sicher zu betrachten ist (siehe A.NK.phys_Schutz sowie A.NK.Admin_EVG)

LS11 Eine Schnittstelle zum Auslösen des Werksreset (via PS7). Im Folgenden werden keine Bedrohungen in Bezug auf diese Schnittstelle betrachtet, da die Schnittstelle aufgrund der Annahmen an die Zugänglichkeit als sicher zu betrachten ist (siehe A.NK.phys**_Schutz** sowie A.NK.Admin_EVG)

Anwendungshinweis 13: Der EVG bietet eine Schnittstelle für entferntes Management entsprechend der Konnektor-Spezifikation [17], Abschnitt 4.3.8, an.

Das lokale und entfernte Management des Netzkonnektors erfolgt über die LAN- bzw. WAN-Schnittstellen (LS6 via PS2 und LS8 via PS3) die vom Netzkonnktor bereitgestellt werden. Über diese Schnittstellen wird das Management-Modul des Anwendungskonnektors angesprochen. Dieses übernimmt die Ablaufsteuerung. Das Management-Modul ruft die entsprechenden Managementfunktionen des Netzkonnektors über die Schnittstelle LS1 auf. Die Authentisierung des Administrators wird durch den Netzkonnektor umgesetzt.

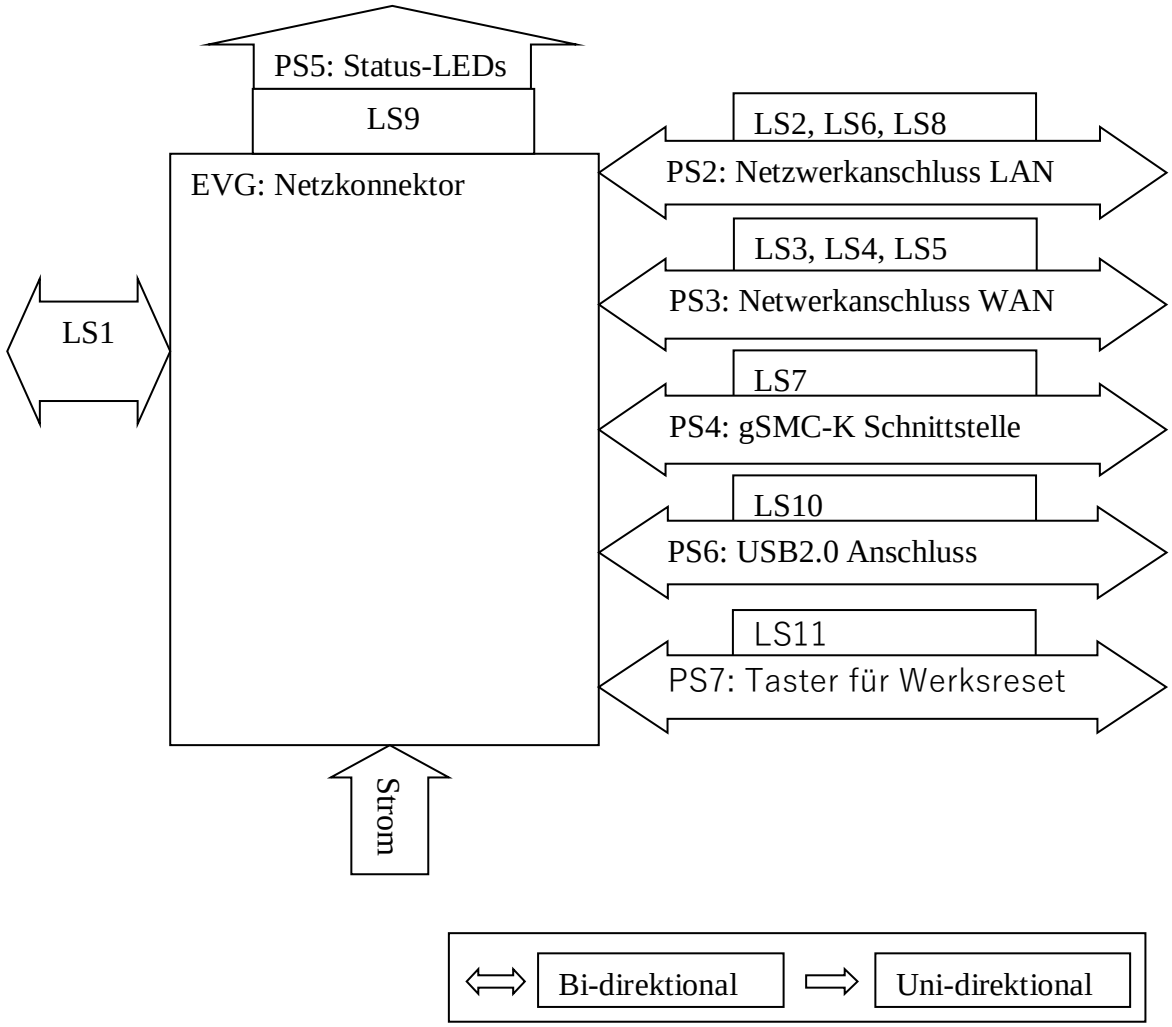

Abbildung 3: Konnektor: externe, physische und logische Schnittstellen

1.3.4. Aufbau und physische Abgrenzung des Netzkonnektors

Eine grobe Abgrenzung des Netzkonnektors von den übrigen Teilen des Konnektors erfolgte bereits in Abschnitt 1.3.

Anwendungshinweis 14: Die Abbildung 4, Abbildung 5 und Abbildung 6 stellen das allgemeine Architekturkonzept des gesamten Konnektors dar. Hieraus wird die Einordnung des EVG ersichtlich.

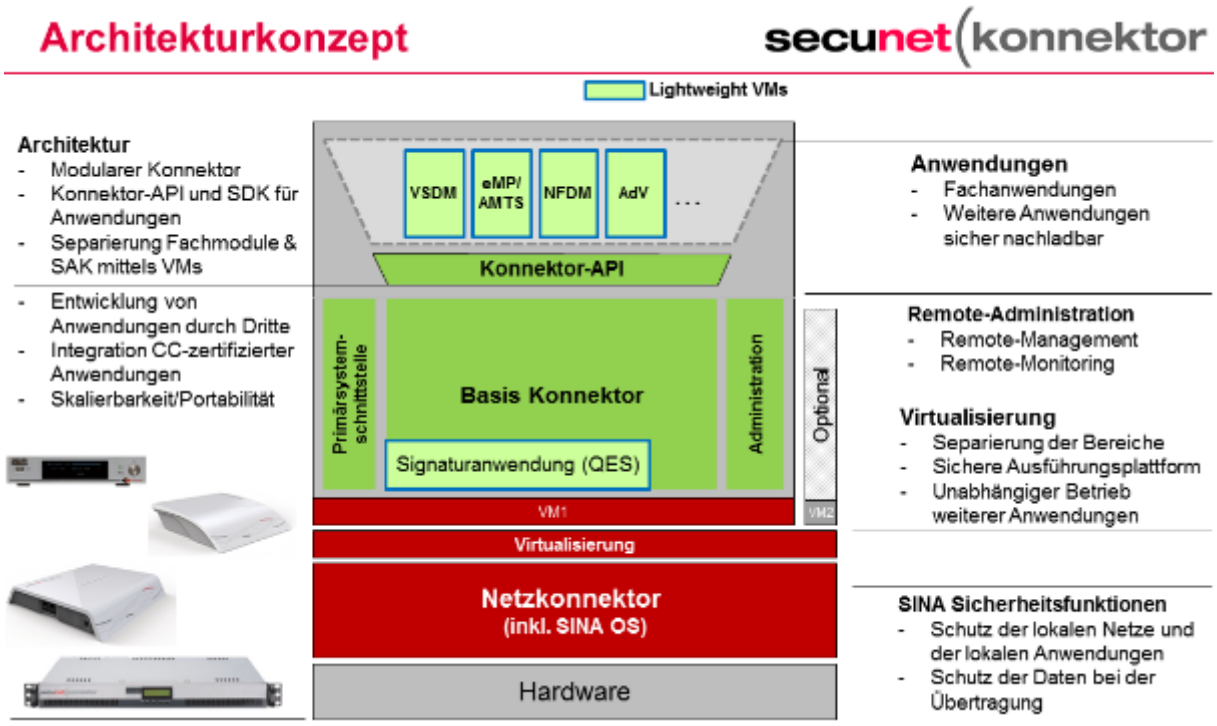

Abbildung 4: Konnektor Architekturkonzept (schematisch)

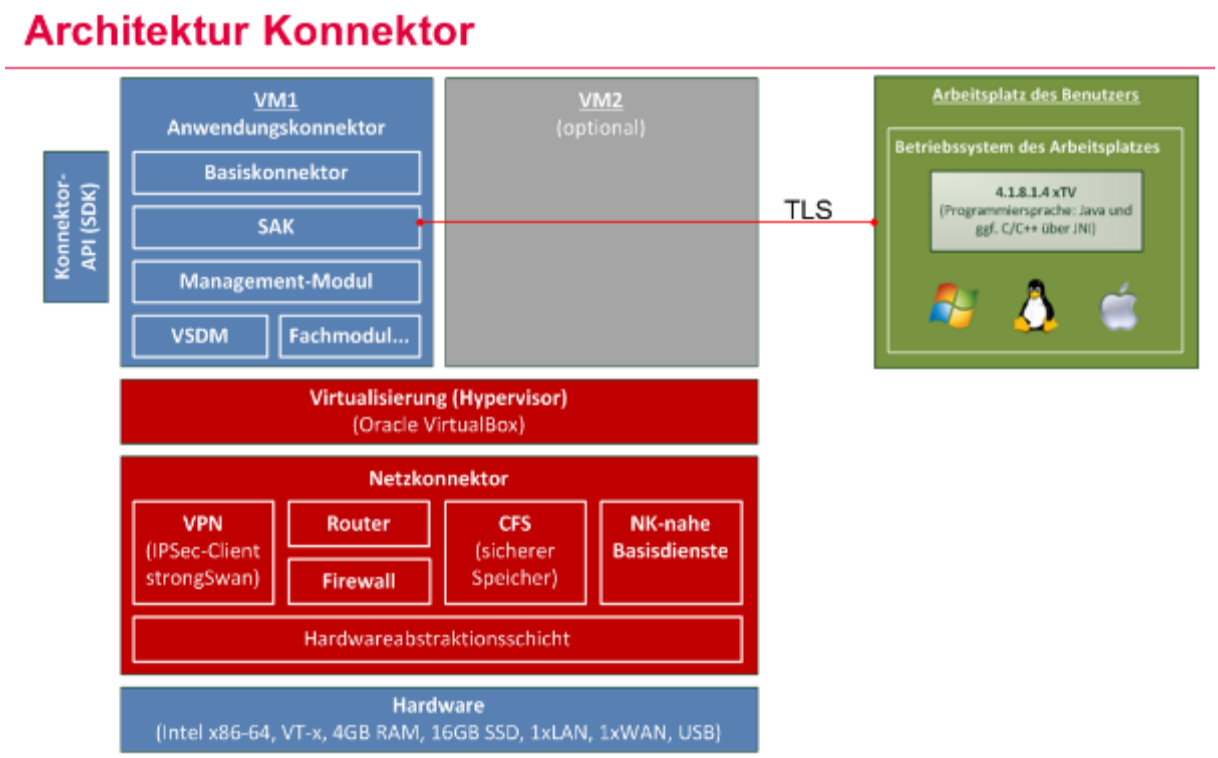

Abbildung 5: Konnektor Architektur Komponentenansicht (schematisch)

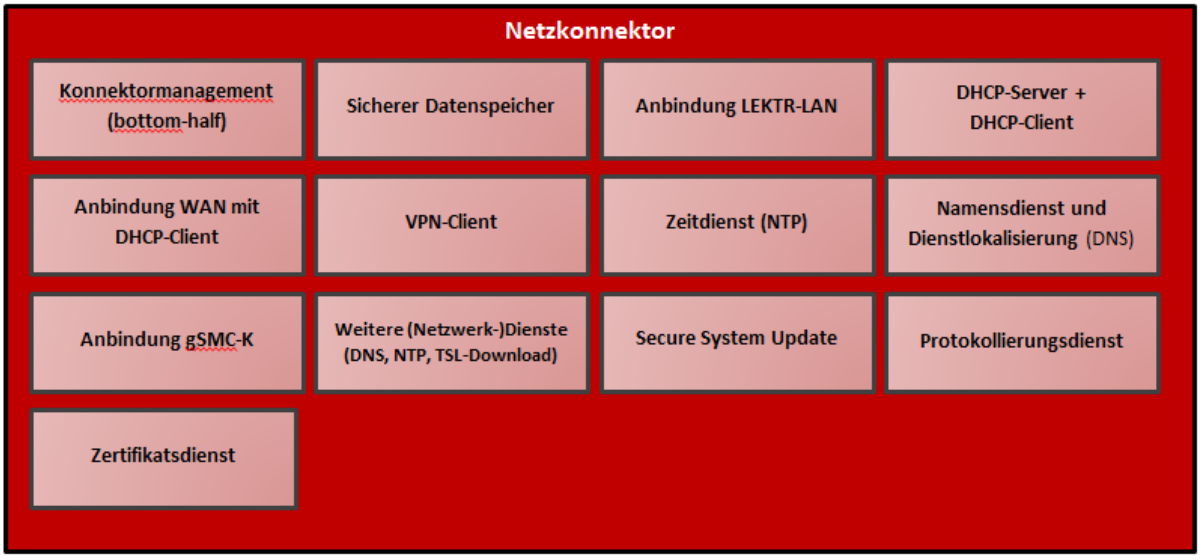

Abbildung 6: Netzkonnektor Komponenten

Architekturübersicht

- Die Hardware stellt die Basis des Netzkonnektors dar. Die Funktionalität der Hardware wird aus dessen Sicht als IT-Umgebung betrachtet (z. B. stellt diese die Echtzeituhr im Sinne von OE.NK.Echtzeituhr bereit). Diese Plattform des Konnektors stellt dem EVG eine Ausführungsumgebung zur Verfügung, die die von ihm verarbeiteten Daten vor dem Zugriff durch Dritte (andere Programme, Prozesse, IT-Systeme o. ä.) schützt. Die Funktionalität der Hardware ist nicht Teil des EVG.

- Der Netzkonnektor basiert auf SINA-OS. Es besitzt einen speziell von secunet in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gehärteten Linux-Kernel. Dieser bildet mit seinen Gerätetreibern die Hardwareabstraktionsschicht und setzt direkt auf der Hardware auf. Weiterhin enthält der Linux- Kernel des SINA-OS Anteile des VPN Clients, stellt die Routing- und Firewall- Funktionen des Netzkonnektors bereit und bindet ein Cryptographic File System (CFS) als sicheren Speicher ein. Auf dem SINA-OS läuft eine spezielle Oracle VirtualBox als Hypervisor, die eine virtuelle Maschine (VM1) als Ausführungsumgebung für den Anwendungskonnektor bereitstellt. Zudem sind die Dienste des Netzkonnektors im Basissystem (SINA-OS) beheimatet. Die beschriebene Funktionalität bildet den EVG.

- Die virtuelle Maschine VM1 enthält den Anwendungskonnektor, der aus Basiskonnektor, Management-Modul und den Fachmodulen besteht. Weiterhin ist die Signaturanwendungskomponente (SAK) in dieser VM beheimatet. Der Fachmodulkonnektor ergibt sich aus den für Fachmodule vorgesehenen Schnittstellen des Basiskonnektors und des Netzkonnektors. Als Betriebssystem in VM1 kommt ein minimalisiertes Linux zum Einsatz. Die virtuelle Maschine VM2 ist optional und für Erweiterungen vorgesehen. Die beschriebene Funktionalität ist nicht Teil des EVG.

- Für die Entwicklung weiterer Fachmodule wird ein ‚Konnektor-API' (linke Seite in Abbildung 5) als Schnittstelle standardisiert. Diese bietet die Funktionen des Fachmodulkonnektors (und damit auch des Basiskonnektors), der SAK und des Management- Moduls an. Bis auf den Ablageort der digital signierten Konnektor-Firmware ist der gesamte Persistenzspeicher des Konnektors durch das vom Netzkonnektor bereitgestellte CFS verschlüsselt. Die beschriebene Funktionalität ist nicht Teil des EVG.

Alle benannten Teile des Konektor befinden sich wie in Abbildung 2 angezeigt innerhalb eines Gehäuses. Die physische Abgrenzung des Netzkonnetors 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 [17] definierten Schnittstellen weitgehend automatisch. Die Abbildung 6 zeigt die architektonische Aufteilung der im Folgenden beschreibenden Sicherheitsdienste des Netzkonnektors.

Anwendungshinweis 15: **Authentisierung des Administrators:** Der EVG sieht einen gemeinsamen Administrator-Account für NK und AK vor. Die Authentisierung des Konnektor-Administrators wird dabei vom NK vorgenommen. Der NK setzt nach erfolgreicher Authentisierung den Authentisierungszustand und autorisert auf diese Weise die Zugriffe des Administrators. Es wird keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) durchgeführt. Der Authentisierungszustand ist Aufgrund der Annahme A.NK.phys_Schutz vor Manipulation abgesichert.

Anwendungshinweis 16: **Vollständigkeit der Dienste:** Die Dienste des EVGs wurden aus NK-PP [12] übernommen und entsprechend der dort verankerten Freiheitsgrade präzisiert.

Anwendungshinweis 17: **Transaktionssicherheit:** 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 gemäß NK-PP [12] folgende Sicherheitsdienste:

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 erzwingt die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen und verbietet ungeschützten Zugriff auf das Transportnetz. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[5], 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[6] sowie Verbindungen zum CRL Download Server.

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 kommt daran, die Integrität des Konnektors zu bedrohen.

Anwendungshinweis 19: Der Netzkonnektor enthält kein **Application Layer Gateway**. Der Anwendungskonnektor wird 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.

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

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

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: Der EVG implementiert eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK (Siehe auch Konnektor-Spezifikation [17], Anforderung 352 TIP 1 A 4788). Die Zeitsynchronisation erfolgt ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform, 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 Anwendungskonnektor (LS1) die Funktion eines DNS-Servers zur Verfügung.

Gültigkeitsprüfung von Zertifikaten: Der EVG überprüft die Gültigkeit der Zertifikate des Kommunikationspartners, die für den Aufbau eines VPN-Kanals verwendet werden.[7] 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 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: Der EVG führt keine explizite Prüfung der Algorithmen auf deren Gültigkeit gegenüber den Vorgaben in TR-03116-1[14] durch. Die Verwendung von gültigen Algorithmen wird durch das Aufbringen eines korrekten und evaluierten Softwarestandes des EVG unter Nutzung des sicheren Updatemechanismus sichergestellt.

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:

[7] 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.

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 ist hinreichend groß dimensioniert. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [17].

Anwendungshinweis 24: Eine (über die Anforderungen der Konnektorspezifikation [17] hinausgehende) Auswertung des Sicherheits-Logs durch den Netzkonnektor erfolgt nicht.

Anwendungshinweis 25: Die geschützte Speicherung des Protokolls (u. a. zyklisches Überschreiben, Schutz gegen Manipulation durch den Administrator) wird als übergreifende Funktionalität im PP [11] gefordert (siehe dort, FAU_STG.1/AK und FAU_STG.4/AK).

Administration: Der EVG ermöglicht ein Management (Administration) nach Autorisierung des Administrators. Der Konnektor setzt eine übergreifende Adminsitratorrolle um. Die Authentisierung des Konnektor-Administrators wird vom Netzkonnektor vorgenommen.

Der EVG bietet eine lokale und entfernte Managementschnittstelle an.

Anwendungshinweis 26: Der EVG bietet die Möglichkeit eines sicheren SW/FW/Konfigurations- und TSL-Updates über die Managementsschnittstellen an. Weitere Managementfunktionen werden gemäß FMT_MTD.1.1/NK umgesetzt.

Eine Möglichkeit zur Fernwartung ist gemäß Konnektor-Spezifikation [17], Abschnitt 4.3 implementiert. Zur Absicherung der Fernwartung werden dieselben Mechanismen verwendet wie zur Absicherung der lokalen Administration an der LAN-Schnittstelle (sicherer Kanal zwischen Administrator-Arbeitsplatz und Netzkonnektor siehe FTP_TRP.1/NK.Admin, Autorisierung des Administrators siehe FIA_UAU.1/NK.SMR). Es ist jedoch zu beachten, dass laut Konnektorspezifikation (Kapitel 4.3.8) bei einer Managementverbindung über die WAN Schnittstelle der Verbindungsaufbau immer vom Konnektor ausgeht.

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

1.3.6. Non-EVG hardware/software/firmware

Der EVG ist die Software des Netzkonnektors Anteils inklusive UEFI Secure Boot Firmware für einen Einbox-Konnektor.

Anwendungshinweis 27: Die Hardware ist nicht Teil des EVGs

Die Hardware des Einbox-Konnektors ist eine komplett geschlossene, passiv gekühlte Appliance ohne Lüftungsöffnungen mit externem Netzteil. Das Gehäuse besitzt die in Kapitel 1.3.3.1 beschriebenen physischen Schnittstellen, insbesondere RJ45-Ports für WAN und LAN Verbindungen, USB-Ports für die Notfall-Administration und LEDs für die Signaleinrichtung. Im Gehäuse sind die gSMC-Ks des Konnektors verbaut. Als gSMC-Ks werden folgende von der gematik zugelassene gSMC-Ks verwendet:

STARCOS 3.6 Health SMCK R1
TCOS Security Module Card - K Version 2.0 Release 1
STARCOS 3.7 gSMC-K R1
TCOS Security Module Card – K Version 2.0 Release 2

verwendet. Je Einbox-Konnektor werden dabei immer identische gSMC-Ks verbaut, die anhand der Identifikationsnummer (ICCSN) ermitteln werden können (siehe Handbuch [52]). 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 WAN/LAN
Smartcard-Leser (für gSMC-K)	3 interne Smartcard-Leser für ID-000 Karten
RTC	Real Time Clock mit max. Drift von +/- 20ppm

Tabelle 2: 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.

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 eine „**strict conformance**“ Konformität zum „Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097“, [12].

2.3. Paket-Konformität

Das Security Target strebt 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) an.

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).

Da das Security Target keine Konformität zu einem anderen Schutzprofil behauptet, können auch keine Widersprüche zwischen 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 werden die Komponenten ADV_IMP.1 und ALC_TAT.1 aufgenommen und die Komponenten ADV_TDS.3 und ADV_FSP.4 augmentiert. 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.

2.5. ST-Organisation

Der Aufbau dieses Security Targets folgt der Gliederung, des zugehörigen Schutzprofils („Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP, [12]), BSI-CC-PP-0097“.

3. Definition des Sicherheitsproblems

In diesem Abschnitt wird zunächst beschrieben, welche Werte der EVG schützt, welche externen Einheiten mit ihm interagieren und welche Objekte von Bedeutung sind. Auf dieser Basis wird danach beschrieben, welche Bedrohungen der EVG abwehrt, welche organisatorischen Sicherheitspolitiken beachtet werden und welche Annahmen an seine Einsatzumgebung getroffen werden.

Die Namensgebung der symbolischen Bezeichner für die im Folgenden definierten Bedrohungen, organisatorischen Sicherheitspolitiken sowie der Annahmen folgt der des zugrundeliegenden PP [12].

3.1. Zu schützende Werte

Werte sind durch Gegenmaßnahmen zu schützende Informationen oder Ressourcen. Der Schutz kann durch den EVG 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[8] 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 dem 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.

3.1.1. Primäre Werte

Die primären Werte sind in der folgenden Tabelle 3 aufgeführt.

[8] 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.

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 Telematikinfrastruktur-Plattform (beide Übertragungsrichtungen)	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.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 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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		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 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 Telematik-infrastruktur-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 3: Primäre Werte

Die primären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 1 aus dem PP [12]

3.1.2. Sekundäre Werte

Die sekundären 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 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 Kommunikations-partners sicherzustellen. ⇒ 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 über-tragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungs-geheimnissen (z. B. Passwort für Administrator-authentisierung, 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. Dies gilt insbesondere auch für die Zertifikate der gSMC-K für die Laufzeitverlängerung.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
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). Dies gilt insbesondere auch für die Zertifikate der gSMC-K für die Laufzeitverlängerung.
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_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 Erzeugung von Zeitstempeln in Sicherheits-Log-Daten oder Audit-Daten verwendet. ⇒ T.NK.TimeSync

Tabelle 4: Sekundäre Werte

Die sekundären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 2 aus dem PP [12].

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[9] 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,

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

NK-Admin oder auch **NK-Administrator**: Administrator des Netzkonnektors,

Angreifer ein Angreifer.

Der NK-Admin authentisiert sich gegenüber dem Konnektor (siehe O.NK.Admin_EVG). Der EVG unterscheidet intern zwischen den drei Administrator-Rollen *local administrator*, *remote administrator* und *super administrator*. Siehe auch Anwendungshinweis 38:.

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

[9] 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.*

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.
O_LZV_Zert_gSMCK	Zertifikate für die Laufzeitverlängerung • C.SAK.AUT • C.NK.VPN • C.AK.AUT • C.SAK.AUTD_CVC • C.SMC.AUT_CVC

Die Zertifikatstypen (ECC-256, ECC-384, RSA-2048) der vom Trusted Service Provider für den Konnektor zur Verfügung gestellten erneuerten Zertifikate, hängen jeweils von den in der gSMC-K hinterlegten Zertifkaten 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 [12], Abschnitt 3.3.1 zu entnehmen.

Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen sind:

- 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 Leistungserbringer 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 Leistungserbringer 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.

Schließlich erlaubt der EVG lokale und entfernte Administration, die ebenfalls das Ziel von Angriffen sein kann (siehe T.NK.local_admin_LAN und T.NK.remote_admin_WAN).

3.3.2. Liste der Bedrohungen

Die folgende Abbildung 7 zeigt die beschriebenen externen Einheiten, Objekte und Angriffspfade (nummerierte Pfeile) im Zusammenhang.

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt. Das Kästchen „LAN-Interface“ schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

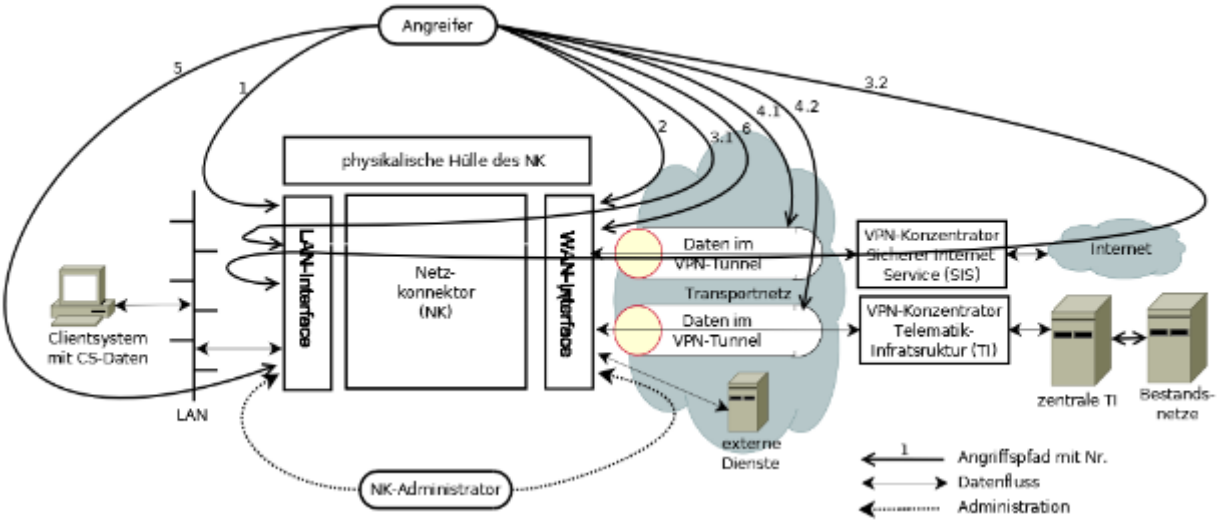

Abbildung 7: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 7 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 5: Kurzbezeichner der Bedrohungen

In den folgenden Abschnitten werden die Bedrohungen genauer beschrieben. Die Definitionen wurden aus NK-PP [12] übernommen.

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[10] 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 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.[11] Ziel bzw. Motivation des Angriffs ist es, den Netzkonnektor zu kompromittieren, um

- im Netzkonnektor gespeichertes kryptographisches Schlüsselmaterial, Management-Daten, Authentisierungsgeheimnisse und zu schützende Daten der TI und der Bestandsnetze im EVG 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.

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

[11] 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.

Für diesen Angriff kann der Angreifer sowohl vorhandene IT-Systeme im LAN des Leistungserbringers nutzen als auch eigene (z. B. Notebook, Netbook, PDA[12], 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.

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 (vgl. Abbildung 2 in Abschnitt 1.3.2).

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 7 zwei Angriffspfade unterschieden:

[12] Personal Digital Assistant

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[13] 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 EVG
- kryptographisches Schlüsselmaterial
- Authentisierungsgeheimnisse
- Management-Daten (während ihrer Speicherung im EVG)
- 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 (vgl. Abbildung 2 in Abschnitt 1.3.2).

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

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

aus Abbildung 7) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 7) 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

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). 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.
- 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[14]. 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.

Anmerkung: Die Tatsache, dass ein Angreifer gefälschte Netzkonnektoren in Umlauf bringt, ist gleichbedeutend mit dem In-Umlauf-Bringen gefälschter Konnektoren, da der EVG in einer Einbox-Lösung integriert ist.

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-Verteilungspunktes manipulieren oder sich selbst als dieser Verteilungspunkt ausgeben. Der Angreifer verfügt über hohes Angriffspotential.

[14] 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.

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 schützende 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 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 [19]. 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 an den Leistungserbringer und die 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 bereitgestellt werden. Der Administrator hat im Zertifizierungsfall darauf zu achten, dass nur die gemäß dem Zertifizierungsreport ausgewiesenen technischen Komponenten zum Einsatz kommen.

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[15]). 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: Mit OSP.NK.SW-Update wurde die Organisatorische Sicherheitspolitik OSP.SW-Update aus dem Protection Profile BSI-CC-PP-0098 [11] des Gesamtkonnektors übernommen.

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 physischen 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

[15] Einspielen älterer Software-Versionen ist nur dann erlaubt, wenn die einzuspielende Version in der aktuell gültigen Liste zulässiger Software-Versionen (Firmware-Gruppe) ist.

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: Nicht relevant. 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: Der Beitrag des EVG zur Abwehr von Denial of Service Angriffen besteht lediglich darin, dass nur autorisierten Benutzern Zugang zu den Diensten der Telematikinfrastruktur vermittelt wird. Zudem trägt die Verwendung von DNSSEC bei der Ermittlung von IP-Adressen der VPN Konzentratoren TI und SIS zur Abwehr von DoS Angriffen bei. Insofern kann der Netzkonnektor die Abwehr von Denial of Service Angriffen unterstützen, aber nicht die alleinige Verantwortung dafür übernehmen. Die Verantwortung für den Schutz der Systeme der zentralen Telematikinfrastruktur-Plattform liegt bei den Firewall-Systemen im Perimeter der zentralen Telematikinfrastruktur-Plattform. Der Schwerpunkt der Abwehr durch den EVG liegt bei den in O.NK.PF_WAN und O.NK.PF_LAN beschriebenen Bedrohungen.

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 EVG implementiert einen Paketfilter und stellt separate Kommunikationskanäle für Daten, welche zu schützende Daten der TI *und der Bestandsnetze* sind (z. B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur-Plattform) und entsprechend gekennzeichnet sind zur Verfügung. Basierend auf der Informationsflusskontrolle wertet der Paketfilter die IP Information aus, welche über die logischen Schnittstellen ausgetauscht wird.

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 EVG implementiert einen Paketfilter und stellt separate Kommunikationskanäle für Daten, welche zu schützende Daten der TI *und der Bestandsnetze* sind (z. B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur-Plattform) und entsprechend gekennzeichnet sind zur Verfügung. Basierend auf der Informationsflusskontrolle wertet der Paketfilter die IP Information aus, welche über die logischen Schnittstellen ausgetauscht wird.

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 [11] 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 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 Schutzprofil [11] als übergreifende Sicherheitsfunktion modelliert.

4. Sicherheitsziele

Die Namensgebung der symbolischnen Bezeichner für die im Folgenden definierten Sicherheitsziele folgt der aus dem zugrundeliegenden dem PP [12].

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 sich selbst.

4.1.1. Allgemeine Ziele: Schutz und Administration

O.NK.TLS_Krypto 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 [19]. 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. Im vorliegenden ST für den Netzkonnektor geht es lediglich darum, die kryptographische Grundfunktionalität für TLS so zur Verfügung zu stellen, dass sie gegen hohes Angriffspotential geschützt ist. Dies dient dem Selbstschutz des Konnektors als Ganzes und soll aus diesem Grund nach AVA_VAN.5 evaluiert werden.

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 schützt die *TSF Daten* (den ausführbaren Code) auf der Basis von geeigneten kryptographischen Signaturen unter Nutzung von Vorgaben gemäß TR-03116-1 [14].

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 ermöglicht 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 nur die Rolle Administrator. Dabei werden im EVG die Administrator-Rollen *local administrator*, *remote administrator* und *super administrator* unterschieden. Der lokale und Remote Administrator können den EVG jeweils über einen entsprechenden Port an der LAN-Schnittstelle konfigurieren. Der Super Adminsistrator benutzt die gleiche Schnittstelle wie der lokale Administrator und kann zudem Benutzerkonten verwalten und Zugriffsrechten vergeben. Es können alle Management-Funktionen der TSF von den drei Administratoren ausgeführt werden. Daher werden unter dem Subjekt Administrator in den SFRs die einzelnen Rollen zusammengefasst.

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

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

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 muss durch den Administrator erfolgen.

Hinweis: O.NK.Update wurde von O.Update aus dem Protection Profile BSI-CC-PP-0098 [11] des Gesamtkonnektors abgeleitet. Der hier beschriebene Update-Vorgang für die Software des EVG bezieht sich auf die Software des Konnektors, die Updatefunktion für Software wird komplett durch den Netzkonnektor implementiert. Die Updatefunktion für Software kann auch für das Nachladen von geprüften und freigegebenen Fachmodulen verwendet werden.

O.NK.Admin_Auth Authentisierung des Administrators

Der EVG führt selbst die Authentisierung des Administrators durch.

Hinweis: Das Sicherheitsziel *OE.NK.Admin_Auth* für die Umgebung aus dem zugrundeliegendem Protection Profile [11] wurde in ein Sicherheitsziel O.NK.Admin_Auth für den EVG umgewandelt, siehe auch Anwendungshinweis 54:.

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 Authentifizierung seiner selbst gegenüber den VPN-Konzentratoren in der zentralen Telematikinfrastruktur-Plattform und des SIS.

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

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

geeignete Algorithmen Außerdem überprüft der EVG, dass die verwendeten Algorithmen gemäß *Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte für der* Bundesregierung, Teil 1: Telematikinfrastruktur [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [19] noch gültig sind.

Anwendungshinweis 44: Der EVG implementiert die Algorithmen TR-03116-1 [14] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [19]. Eine Prüfung der Gültigkeit der Algorithmen wird nicht explizit durchgeführt. Dies wird implizit im Rahmen der Evaluierung des Netzkonnektors sichergestellt. Weiterhin bietet der EVG keine Funktionalität die Verfügbarkeit der in Bezug auf die beannnten Spezifikationen ungültigen Algorithmen selektiv einzuschränken. Eine Einschränkung der im Konnektor verwendbaren Algortihmen kann nur über ein Software-Update erreicht werden.

O.NK.Zert_Prüf Gültigkeitsprüfung für VPN-Zertifikate

Zertifikate prüfen

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[16] 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.

4.1.3. Ziele für die Paketfilter-Funktionalität

O.NK.PF_WAN Dynamischer Paketfilter zum WAN

WAN-seitiger Paketfilter

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

[16] Der Begriff „Nutzdaten“ schließt in diesem Security Target 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.

Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt[17], 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

LAN-seitiger Paketfilter

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.

VPN-Tunnel erzwingen

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.

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

[17] Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [17], Kapitel 2.7.

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

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

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 des Konnektors muss eine Real Time Clock mit maximal zulässigem Drift von +/- 20ppm (part per million) zur Verfügung stellen (siehe Kapitel 1.3.6). 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.

EVG-Identität in gSMC-K 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.

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

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

Anwendungshinweis 49: Der Konnektor verwendet nur von der gematik zugelassene gSMC-K, siehe 1.3.6.

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).

Sensitive Daten sowie die Konfigurations- und Protokolldaten eines Konnektors werden auf einem verschlüsselten Dateisystem (CFS) unter Verwendung eines geräteindividuellen Schlüssels abgelegt. Der Schlüssel dieses CFS wird mit privaten schlüsseln die in einem geschützten Bereich auf der gSMC-K abgelegt sind verschlüsselt.

Anwendungshinweis 50: Der EVG verwendet als sicheren Schlüsselspeicher die gSMC-K. Darin sind auch die privaten Schlüssel zur Entschlüsselung des geräteindividuellen CFS-Schlüssels abgelegt. Die Sicherheit der im CFS abgelegten Daten ist damit wieder auf den sicheren Schlüsselspeicher der gSMC-K zurückzuführen.

Anwendungshinweis 51: Sensitive Daten (z. B. VPN oder TLS session keys, Administrator Passwörter, DNSSEC Vertrauensanker) werden im CFS abgelegt. Die öffentlichen Prüfschlüssel zur Verifikation der eigenen Integrität (secure boot) sind in der FW/SW hardcodiert. Diese werden auch zur Verifikation der Authentizität von Software-Updates verwendet. Es ist (abgesehen vom CFS) kein eigener Schlüsselspeicher implementiert.

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 abhanden kommt, 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 verfügt zur Identifikation über eine eindeutige Seriennummer. 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, so dass weitergehende Schritte (z. B. Sperrung des zugehörigen Zertifikats) eingeleitet werden können.

OE.NK.Admin_Auth aus PP [12] ist für den EVG nicht relevant, da der EVG die Authentisierung des Administartors selbst durchführt, siehe O.NK.Admin_Auth und Anwendungshinweis 54:

Anwendungshinweis 54: Der Konnektor setzt eine übergreifende Administratorrolle um. Die Authentisierung des Konnektor-Administrators wird dabei vom Netzkonnektor vorgenommen. Das Umgebungsziel OE.NK.Admin_Auth des PP [12] wurde in das EVG-Ziel O.NK.Admin_Auth umgewandelt. Die funktionale Anforderung FMT_MSA.4/NK PP [12] wurde nicht in diesem ST übernommen, dafür wurde mit FIA_UAU.1/NK.SMR eine die Authentisierung des Administrators modellierende Anforderung in das ST aufgenommen.

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

PKI-Betrieb, 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.

VPN-Konzentr. sperren

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.

EVGs sperren

Meldet ein Konnektor-Betreiber seinen Konnektor und/oder dessen Sicherheitsmodul gSMC-K als gestohlen oder anderweitig abhanden gekommen, 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.

Anwendungshinweis 55: Siehe auch A.NK.phys_Schutz resp. O.NK.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:

sichere Admin. AK	Er administriert die Anwendungskonnektoren in sicherer Art und Weise.
Schnittstellennutzung	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 Clientsystems

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

sichere Produkte	Er setzt nur Clientsysteme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.
sichere Admin. CS	Er administriert die Clientsysteme in sicherer Art und Weise.
Schnittstellennutzung	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.

keine Schadsoftware — 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.

Internet-Anbindung — 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.

Verantwortung — 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.[18]

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-Konzentrator[19] 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.

[18] 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 Schutzprofil wird daher eine Kombination aus einem gesicherten Zugangspunkt zum Internet (OE.NK.SIS) und lokalen Schutzmaßnahmen auf den Clientsystemen (OE.NK.Betrieb_CS) gefordert.

[19] Laut Konnektor-Spezifikation (Kapitel 2.7) [17] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

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: Mit OE.NK.SW-Update wurde das Sicherheitsziel für die Umgebung OEP.SW-Update aus dem Protection Profile BSI-CC-PP-0098 [11] des Gesamtkonnektors übernommen.

4.3. Erklärung der Sicherheitsziele (Security Objectives Rationale)

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

Die folgende Tabelle 6 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_Authenicity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.Admin_Auth	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	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.gSMC-K	OE.NK.KevStorage	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	X	
T.NK.remote_VPN_Data						X			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			X		X					X	
T.NK.remote_admin_WAN		X		X	X	X		X								X	X	X		X			X							X	
T.NK.counterfeit			X																X						X					X		
T.NK.Zert_Prüf					X	X				X						X			X					X						X		
T.NK.TimeSync					X	X			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																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						
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 6: 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: Die Inhalte in Tabelle 6 und im folgenden Erklärungstext (Abschnitte 4.3.1 und 4.3.2) wurden aus dem NK-PP [12] übernommen. Hierbei wurden die optionalen Zuordnungen, im NK-PP markiert durch (x), entsprechend übernommen oder entfernt.

4.3.2. Abwehr der Bedrohungen durch die Sicherheitsziele

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 6 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.

Optional kann auch O.NK.Stateful bei der Abwehr von T.NK.local_EVG_LAN unterstützen, indem sicherheitsrelevante Ereignisse protokolliert werden. Siehe auch Anwendungshinweis 57:.

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, OE.NK.Echtzeituhr 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.Echtzeituhr, 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 2) 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.

Optional kann auch O.NK.Stateful bei der Abwehr von T.NK.remote_EVG_LAN unterstützen, indem sicherheitsrelevante Ereignisse nicht nur – wie bei T.NK.remote_EVG_WAN – an der WAN-seitigen Schnittstelle, sondern auch an der LAN-seitigen Schnittstelle protokolliert werden (Schreiben von Audit-Daten zur späteren Auswertung mit dem Ziel zustandsgesteuerter Filterung). Siehe auch Anwendungshinweis 57:.

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.Echtzeituhr, OE.NK.Zeitsynchro, OE.NK.KeyStorage, OE.NK.Ersatzverfahren und OE.NK.RNG zur Abwehr der Bedrohung bei.

Anwendungshinweis 58: O.NK.Protokoll (Sicherheits-Log) wird im ST nicht bei der Abwehr von T.NK.remote_VPN_Data berücksichtigt. Siehe auch Anwendungshinweis 57:.

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 die 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. Für die Administration wird ein sicherer TLS Kanal aufgebaut. Hinsichtlich der dabei verwendeten kryptographischen Verfahren trägt OE.NK.Ersatzverfahren zur Abwehr von T.NK.local_admin_LAN bei. Durch OE.NK.phys_Schutz ist der Kommunikationskanals zwischen dem EVG und weiteren Komponenten des Konnektors vor Manipulationen geschützt.

Anwendungshinweis 59: Im Rahmen der Administration kommen kryptographische Verfahren zum Einsatz (Implementierung eines sicheren Kanals). Damit trägt auch OE.NK.Ersatzverfahren zur Abwehr von T.NK.local_admin_LAN und T.NK.remote_admin_WAN bei. OE.NK.phys_Schutz trägt zur Abwehr von T.NK.local_admin_LAN beitragen, da durch den Schutz des Kommunikationskanals zwischen dem EVG und weiteren Komponenten des Konnektors Manipulationen am Gerät verhindert werden können. Siehe auch Anwendungshinweis 57: (Anpassung des Security Targets bei Bedarf).

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 und Anwendungshinweis 59:. 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.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro O.NK.Schutz und OE.NK.KeyStorage bei sowie optional auch OE.NK.PKI und OE.NK.Ersatzverfahren.

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. Im Rahmen der Gültigkeitsprüfung von Zertifikaten werden Plausibilitätsprüfungen durchgeführt, welche die Echtzeit des EVG verwenden; somit trägt auch O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro zur Abwehr von T.NK.Zert_Prüf bei. Zudem trägt auch O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr von T.NK.Zert_Prüf bei, da fehlgeschlagene oder erfolgreiche Updates der Sperrlisten protokolliert werden. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der gSMC-K gespeichert sind, daher unterstützt OE.NK.gSMC-K bei der Abwehr von T.NK.Zert_Prüf. Ein externer Zufallszahlengenerator (OE.NK.RNG) wird darüber hinaus als Lieferant für gute Zufallszahlen genutzt, die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen. Bei T.NK.Zert_Prüf kommen kryptographische Verfahren zum Einsatz, daher trägt OE.NK.Ersatzverfahren zur Abwehr bei.

Anwendungshinweis 60:.O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, O.NK.Protokoll, OE.NK.gSMC-K und OE.NK.RNGtragen zur Abwehr von T.NK.Zert_Prüf bei.

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. Zudem trägt O.NK.Protokoll zur Abwehr der Bedrohungen bei, da erfolgreiche oder fehlgeschlagene Zeitsynchronisation protokolliert wird.

Anwendungshinweis 61: O.NK.Protokoll, OE.NK.gSMC-K, OE.NK.RNG, OE.NK.PKI und OE.NK.Ersatzverfahren tragen zur Abwehr von T.NK.TimeSync bei.

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[20]. 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.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 einerseits durch Erkennungsmechanismen im SIS verhindert werden,

[20] 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.

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).

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.VPN_Auth, 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, SAK) 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 NK-PP, BSI-CC-PP-0097 [12], 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, gegeben. Das Schutzprofil basiert auf Version 3.1 Revision 5 der Common Criteria; diese Version [2] liegt in englischer Sprache vor. Operationen wurden dabei teilweise in deutscher Sprache ausgeführt.

Dieses Security Target übernimmt die Formulierungen des Schutzprofils NK-PP [12].

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 Verfeinerung durch **fettgedruckten Text** in der Anforderung hervorgehoben und 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 [12] ausgeführte Auswahl durch unterstrichenen Text in der Anforderung hervorgehoben. Eine durch das PP bzw. durch die CC vorgegebene und im Security Target ausgeführte Auswahl wird zusätzlich durch [eckige Klammern] hervorgehoben. Für die Operationen ist durch eine Fußnote jeweils der Originaltext bzw. der Text des PP [12] angegeben.

Die Operation **Zuweisung** (assignement) wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Security Target werden bereits im PP [12] ausgeführte Zuweisungen durch *kursiven Text* in der Anforderung hervorgehoben. Durch das PP bzw. durch die CC vorgegebene und im Security Target ausgeführte Zuweisungen werden zusätzlich durch [*eckige Klammern*] hervorgehoben. Für die Operationen ist durch eine Fußnote jeweils der Originaltext bzw. der Text des PP [12] angegeben.

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.
- 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 Security Target definierten SFRs wiederverwendet werden..

6.2.1. VPN-Client

VPN

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*[21] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[22] and protection of the channel data from modification *and*[23] disclosure.

FTP_ITC.1.2/NK.VPN_TI The TSF shall permit the TSF[24] to initiate communication via the trusted channel.

[21] refinement

[22] refinement

[23] refinement (or → and)

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

FTP_ITC.1.3/NK.VPN_TI The TSF shall initiate communication via the trusted channel for *communication with the TI*[25].

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 [17], RFC 4301 (IPsec) [28], RFC 4303 (ESP) [31]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [32]) 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)***[26]* that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication***[27]* and protection of the channel data from modification **and**[28] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[29] 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*[30].

---

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

26 refinement

27 refinement

28 refinement (or → and)

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

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

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 [17], RFC 4301 (IPsec) [28], RFC 4303 (ESP) [31]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [32]) 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) [32], siehe [19], 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: Die Kommunikation von EVGs untereinander ist nicht vorgesehen.

Informationsflusskontrolle

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 6.2.8) sichergestellt wird.

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

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)*[31] 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) TSL-Dienstserver

(10) hash&URL server,

(11) registration server of the VPN network provider,

(12) 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)[32].

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:

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

[32] [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_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
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 Bestandnetze (ANLW_BESTANDSNETZE)
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
TSL Diensteserver	IP-Adresse des TSL-Diensteserver Hierzu zählen die Download-Bereiche: CERT_TSL_DOWNLOAD_ADDRESS_INTERNET, CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
	CERT_TSL_IP_ADDRESS_INTERNET CERT_TSL_IP_ADDRESS_INTERNET_BU
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.

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=ENAB LED 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=DISAB LED 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*[33] 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*[34] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES.[35]

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

---

33 [assignment: *information flow control SFP*]

34 IP = Internet Protocol

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

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,

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

d) 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≠"").[36]

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

(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*[37].

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*][38].

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.

---

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

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

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

(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.

(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*] [39].

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“ nach [gemSpec_Kon], TIP1-A_4823 wird vom EVG nicht umgesetzt. Das Attribut

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

MGM_LOGICAL_SEPARATION kann daher nicht auf ENABLED gesetzt werden.
Die Regel FDP_IFF.1.2/NK.PF Regel 4 c) wird auch benutzt um die Operation SendData zum Registrierungsserver zu senden (A_21159).

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 6.2.8) 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 Historie der Verbindung durch die firewall des Betriebsystemkernels (iptables). Es werden eingehende Verbindungen 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] [18], Tabelle 1 aufgeführten Protokolle zulässig. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.

EVG erzwingt, 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 (mittels FDP_IFF.1.3/NK.PF bis FDP_IFF.1.5/NK.PF) ergänzt.

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).

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*[40] to provide restrictive[41] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [*role administrator*][42] 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.

Anwendungshinweis 69: Es gibt nur eine Administrator Rolle welche alternative Default-Werte spezifizieren darf. Dabei wird nicht zwischen lokalem und entfernten Management unterschieden.

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 [23] 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

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

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

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

24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht [*nicht mehr als 330ms*][43] von der Zeitinformation der darüberliegenden Stratum Ebene ab.

Anwendungshinweis 70: Zum Zeitdienst siehe Konnektor-Spezifikation [17], Abschnitt 4.2.5 *Zeitdienst.*

Anwendungshinweis 71: Die im Refinement geforderte Zeitsynchronisation entspricht den Anforderungen der aktuellen Version der Konnektor-Spezifikation [17]. Es wurde keine verschärfung des Refinement aus dem NK-PP [12] vorgenommen.

Anwendungshinweis 72: Gemäß Konnektor-Spezifikation [17], Abschnitt 3.3 *Betriebszustand,* erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [17]

- *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, welche den Betriebszustand an der Außenhaut des Konnektors anzeigt, um die benannte Anforderung der Spezifikation umzusetzen, siehe LS9 und PS5 in Kapitel 1.3.3 sowie die Anforderungen an die Konnektor Hardware in Kapitel 1.3.6.

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*[44] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[45] 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

[43] [selection: *nicht mehr als 330ms*, [assignement: *andere Zeit*]]

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

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

(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 den Anforderumgen der aktuellen Version der Konnektor-Spezifikation [17]. Der EVG führt keine explizite Prüfung der Algorithmen auf deren Gültigkeit gegenüber den Vorgaben in TR-03116-1[14] durch. Die Verwendung von gültigen Algorithmen wird durch das Aufbringen eines korrekten und evaluierten Softwarestandes des EVG unter Nutzung des sicheren Updatemechanismus sichergestellt.

Anwendungshinweis 74: Die TSL und die CRL muss gemäß Anforderung A_4684 in der Konnektor-Spezifikation [17] 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 [17]). Die Liste der entsprechenden Zertifikate aus der TSL wird im Netzkonektor hinterlegt.

6.2.4. Stateful Packet Inspection

Anwendungshinweis 75: 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, es gibt keine komplexe Erkennungslogik für Angriffe.

Der Aspekt der Stateful Packet Inspection wird durch FDP_IFF.1.4/NK.PF modelliert.

6.2.5. Selbstschutz

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[46] 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*][47].

Refinement: Die sensitiven Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In

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

[47] [assignment: *list of objects*]

jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. Reset überschrieben werden.

Anwendungshinweis 76: Der EVG 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).

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][48] to demonstrate the correct operation of [the TSF][49].
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[50].
FPT_TST.1.3/NK	The TSF shall provide authorised users with the capability to verify the integrity of [TSF][51].
Refinement:	Zur Erfüllung der Anforderungen aus FPT_TST.1/NK implementiert der EVG die Mechanismen.1, 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 77: Die kryptographischen Verfahren werden in Software implementiert. Der Benutzer kann die Selftests 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 (Konfigurationsdateien, TSF-Daten) mit kryptographischen Verfahren beim Programmstart.
- Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K als Seed Quelle für den deterministischen Zufallszahlengenerator des TOE (OE.NK.RNG).

[48] [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*]]

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

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

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

Schutz von Geheimnissen, Seitenkanalresistenz

FPT_EMS.1/NK Emanation of TSF and User data

Dependencies: No dependencies.

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)*[52] in excess of *limits that ensure that no leakage of this sensitive data occurs*[53] enabling access to

- *session keys derived in course of the Diffie-Hellman-Keyexchange-Protocol,*
- *[*none*]*[54],
- *[*none*]*[55],
- *[*none*]* [56],
- *[*none*]* [57],
- [*none*][58] and
- *data to be protected ("*zu schützende Daten der TI und der Bestandsnetze")
- [*none*][59].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)[60]* are unable to use the following interface *WAN interface or LAN interface of the connector*[61] to gain access to **the sensitive data (TSF data and user data) listed above**[62].

---

[52] [assignment: *types of emissions*]

[53] [assignment: *specified limits*]

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

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

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

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

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

[59] [assignment: *list of types of user data (may be empty)*]

[60] [assignment: *type of users*]

[61] [assignment: *type of connection*]

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

Anwendungshinweis 78: Es wurden keine weiteren Verfeinerungen vorgenommen. Zur Integritätsprüfung beim Selbsttest und beim Software-Update werden öffentliche Schlüssel verwendet. Die Software Images werden unverschlüsselt übertragen. Die Authentisierung des Administrators wird vom Netzkonnektor durchgeführt. Für die entsprechenden Auswahl Operationen des NK-PPs [12] wurde daher „none“ gewählt.

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][63] 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.*[64]
- **Fehlerzustände according to [17], table 3**.[65]

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:

---

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

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

65 Refinement: Addition of "**Fehlerzustände according to [17], table 3"** to the list of auditable events

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 ST, [*no 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 79: Es werden alle Fehlerzustände die in der Konnektor-Spezifikation [17], Abschnitt 3.3, Tabelle 3 aufgeführt sind 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 wird, dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „start-up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet. Der Protokollierungsdienst als letzter Dienst bei einem Shut-down des EVG beendet wird, dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „*shut down*“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet.

Anwendungshinweis 80: Die benötigte Größe des für das Security Log zu reservierenden Speicherbereichs ist abhängig von der Größe der einzelnen Log-Einträge, von der verwendeten Kodierung und weiteren Produkteigenschaften. Die Hardware des Konnektors muss mindestens 16 GByte Speicher besitzen damit nebem den Software Anteilen von NK und AK ausreichend speicher für Protokolldaten zur Verfügung steht, siehe 1.3.6.

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 81: Der EVG nimmt bei Konfigurationsänderungen durch einen authentisierten Administrator die Identität (Identifikator) des ändernden Administrators in das Sicherheits-Log auf. Es werden keine unterschiedlichen Administrator-Rollen unterstützt.

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*,
- *SIS*,
- *TI*
- *Anwendungskonnektor*[66].

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.

Anwendungshinweis 82: Der EVG unterstützt die Rolle Administrator. Als Sicherheitsattribut „Autorisierungsstatus“des Benutzers „Administrator“ wird das Identifikator-Attribut verwendet. Die Autorisierung wird vom Netzkonnektor duchgeführt. Bei erfolgreicher Autorisierung des Administrator wird das Attribut im EVG gesetzt.

Anwendungshinweis 83: 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 Kommunkation 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

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

FMT_MTD.1.1/NK The TSF shall restrict the ability to [change_default, query, modify, [*activate/deactivate VPN*]][67] the *real time clock, packet filtering rules* [*none*][68] to *the role Administrator*[69].

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

Anwendungshinweis 84: Nur Administratoren dürfen administrieren: Die aufgelisteten administrativen Tätigkeiten können nur von Administratoren ausgeführt werden.

Anwendungshinweis 85: Nur der Administrator darf ein **Deaktivieren der VPN-Verbindung** vornehmen. Die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ wurde in die Liste bei FMT_SMF.1/NK aufgenommen und innerhalb von FMT_MTD.1/NK wurde der Zugriff auf diese Managementfunktion auf den Administrator beschränkt.

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)*[70]

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 86: Die Zuweisung *all actions except for administrative actions (as specified by FMT_SMF.1*/NK*)* aus dem NK-PP [12] wurde unverändert übernommen.

FIA_UAU.1/NK.SMR Timing of authentication

Authentication of Security Management Roles

Dependencies: FIA_UID.1 Timing of identification

Hier erfüllt durch: FIA_UID.1/NK.SMR

---

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

68 [assignment: *list of TSF data*]

69 [assignment: *the authorised identified roles*]

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

FIA_UAU.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)*[71]

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

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

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 [remote, local][72] 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][73].

FTP_TRP.1.2/NK.Admin The TSF shall permit [the TSF, local users][74] to initiate communication via the trusted path.

FTP_TRP.1.3/NK.Admin The TSF shall require the use of the trusted path for *initial user authentication and administrative actions*.[75]

Anwendungshinweis 87: Die Wartung kann über die LAN-Schnittstelle (PS2) und über die WAN-Schnittstelle (PS3) erfolgen. Eine WAN-Verbindung geht immer vom EVG aus, daher ist in FTP_TRP.1.2/NK.Admin der *remote user* nicht aufgeführt.

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.)

---

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

72 [selection: *remote, local*]

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

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

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

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

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.)[76]

- **Aktivieren und Deaktivieren des VPN-Tunnels**[77]

Anwendungshinweis 88: 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*[78] to restrict the ability to [query, modify, [*change_default*]][79] the security attributes *packet filtering rules*[80] to *the roles „Administrator“,* [*no other authorised identified roles*][81].

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

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

[77] refinement: **Aktivieren und Deaktivieren des VPN-Tunnels**

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

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

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

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

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 [17], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [17], 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 [17] 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.

Anwendungshinweis 89: Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [17] definierten Anforderungen.

Anwendungshinweis 90: Der Administrator kann einzelne Filter-Regeln direkt über die Managment-Schnittstelle administrieren. Ebenso ist es möglich Filterregeln als signierte Regelsätze (XML Pakete) über die Managment-Schnittstelle zu übertragen. Die Signaturprüfung findet im EVG statt.

Anwendungshinweis 91: Der Netzkonnektor kann seine Filterregeln abhängig von Ereignissen des Anwendungskonnektors dynamisch anpassen. So gelten standartmäßig sehr restriktive Filteregeln, die zum Beispiel erst beim Aufbau eines VPN Kanals erweitert werden. Einstellungen der Filterregeln durch den Administrator werden dabei niemals überschrieben.

FMT_MSA.4/NK aus PP [12] ist für den EVG nicht relevant, da der EVG die Authentisierung des Administartors selbst durchführt, siehe O.NK.Admin_Auth und Anwendungshinweis 54:. Mit FIA_UAU.1/NK.SMR wurde eine die Authentisierung des Administrators modellierende Anforderung in das ST aufgenommen.

Software Update

Der EVG unterstützt Software Update. Die fogenden SFRs wurden aus dem Protection Profile BSI-CC-PP-0098 [11] des Gesamtkonnektors abgeleitet.

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

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*][82] on

[

- *subjects:*

(1) Administrator

- *objects:*

(1) Update-Pakete

- *operations:*

(1) Installieren

][83]

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

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*][84] to objects based on the following:

[

- *subjects:*

(1) Administrator

- *objects:*

---

82 [assignment: *access control SFP*]

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

84 [assignment: *access control SFP*]

(2) Update-Pakete with security attributes:

a. *Signatur*

b. *Software Version*

]85

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) Der Administrator darf nur Update-Pakete installieren, deren Signatur erfolgreich geprüft wurde.

*(2) Nur der Administrator darf Update-Pakete verwenden, die einer Firmwaregruppe angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist***, siehe Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM]**[86].

]87

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*]88.

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

[

(1) Der EVG darf keine automatische Anwendung (Installation) der Update-Pakete unterstützen.

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

]89

FDP_ITC.1/NK.Update Import of user data without security attributes / Update

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

---

85 [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*]

86 Refinement: **, siehe Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM]**

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

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

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

hier erfüllt durch: FDP_ACC.1/NK.Update

FMT_MSA.3

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_ITC.1.1/NK.Update The TSF shall enforce the *Update-SFP*[90] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/NK.Update The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/NK.Update The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*Die TSF muss die Integrität und Authentizität der importierten Update-Dateien überprüfen.*][91]

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

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: FDP_ITC.1/NK.Update

FDP_UIT.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][92] to [receive][93] user data ~~**in a manner**~~[94] protected from [modification, deletion, insertion][95]

FDP_UIT.1.2/NK.Update The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion][96] has occurred.

---

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

91 [assignment: *additional importation control rules*]

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

93 [selection: *transmit, receive*]

94 refinement

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

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

6.2.7. Kryptographische Basisdienste

Anwendungshinweis 92: Während das Schutzprofil für dieses Security Target davon ausgeht, dass der Zufallszahlegnerator der gSMC-K der Umgebung verwendet wird,implementiert der TOE seinen eigenen, deterministischen Zufallszahlengenerator, der durch die gSMC-K geseeded wird. Dieser RNG erfüllt die Anforderungen an einen DRG.3.

Anwendungshinweis 93: Die SFR der Familie FCS in CC Teil 2 [2] enthalten ein [assignment: *cryptographic algorithm*]. Diese Zuweisungen wurden in den SFR im NK-PP [12] in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI bereits vorgenommen. Die TSF muss die darüberhinausgehenden verpflichtenden Vorgaben der angegebenen Standards soweit sie die angegebenen Algorithmen und Protokollen betreffen implementieren und darf 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 [19] 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 94: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Dabei werden vom EVG auch HW Mechanismen (AES-NI) verwendet sofern diese vom Administrator explizit ausgewählt werden.

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*[97] in accordance with a specified cryptographic algorithm *SHA-1, SHA-256, [none]*[98] and cryptographic key sizes *none*[99] that meet the following: *FIPS PUB 180-4 [26].*[100]

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*[101] in accordance with a specified cryptographic algorithm *HMAC with SHA-256, [none]*[102] and cryptographic key sizes [*256 bit*] [103] that meet the following: *FIPS PUB 180-4 [26], RFC 2404 [34], RFC 4868 [35], RFC 7296 [32].*[104]

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

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

[98] [assignment: *cryptographic algorithm*] -> *SHA-1, SHA-256, [assignment: list of SHA-2 Algorithms with more than 256 bit size]*

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

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

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

[102] [assignment: *cryptographic algorithm*] -> *HMAC with SHA-1, [assignment: list of SHA-2 Algorithms with 256bit size or more]*

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

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

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

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 and performing the RSA or ECC operation* [105]

in accordance with a specified cryptographic algorithm *ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpoolP256r1) and sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[106] and cryptographic key sizes *256 bit and 2048 bit*[107] that meet the following: *RFC 8017 (PKCS#1) [25], FIPS PUB 180-4 [26], Standard TR-03111 [16]*[108].

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*[109] in accordance with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42) or AES-GCM (OID*

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

[106] [assignment: *cryptographic algorithm*]

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

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

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

2.16.840.1.101.3.4.1.46 and OID 2.16.840.1.101.3.4.1.6)[110] and cryptographic key sizes *128 bit and 256 bit*[111] that meet the following: *FIPS 197 [27], RFC 3602 [33], RFC 4303 (ESP) [31], RFC 4106 [51], specification [19]* [112].

FCS_COP.1/NK.IPsec 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.IPsec The TSF shall perform *VPN communication*[113] in accordance with a specified cryptographic algorithm *IPsec-protocol*[114] and cryptographic key sizes *256 bit*[115] that meet the following: *RFC 4301 (IPsec) [28], specification [19]*[116].

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 [*key generation for IPsec Session Keys*][117] and specified cryptographic key sizes

[110] [assignment: *cryptographic algorithm*]

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

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

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

[114] [assignment: *cryptographic algorithm*]

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

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

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

[*128 bit, 256 bit*][118] that meet the following: *specification [19], TR-03116 [14]*[119].

Anwendungshinweis 95: 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 Schutzprofil NK-PP [12] eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols (bzw. Elliptic-curve Diffie–Hellman bei ECC) 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 ist.

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*[120] that meets the following *standard: RFC 7296 [32], specifications [19], TR-02102-3 [13]*[121].

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]

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

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

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

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

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 [*zeroisation*][122] that meets the following: [*none*][123].

Anwendungshinweis 96: 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 dabei mit Nullen überschrieben.

Anwendungshinweis 97: Die Operationen entsprechen den Anforderungen in den Dokumenten [14], [19] und [17]. Es wurden keine weiteren Verfeinerungen der Zuweisungen der Operationen durchgeführt. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle definierten Kryptoverfahren.
Der DH-Exponent für den Schlüsselaustausch weist eine Mindestlänge gemäß [19] auf (mindestens 240 Bit). Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy wurden die Vorgaben aus [19] berücksichtigt.

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Hinweis 1: Die von der Spezifikation geforderten TLS-Verbindungen werden erst im Anwendungskonnektor verwendet. Dieser initiiert die TLS-Verbindungen unter der Verwendung der vom Netzkonnektor zur Verfügung gestellten kryptographischer Algorithmen.

Hinweis 2. Die Absicherung der Administrationsschnittstellen des Netzkonnektors erfolgt mittels TLS. Die SFRs aus dem PP [12] wurden dafür 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**[124] provide**s** assured identification of its end points and protection of the channel data from modification **and**[125] disclosure.

FTP_ITC.1.2/NK.TLS The TSF **must be able to**[126] permit *the TSF or another trusted IT-Product*[127] to initiate communication via the trusted channel.

---

122 [assignment: *cryptographic key destruction method*]

123 [assignment: *list of standards*]

124 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 Authentikation genutzt wird.

125 refinement (or → and)

126 refinement (shall → must be able to)

127 [selection: *the TSF, another trusted IT-Product]*

FTP_ITC.1.3/NK.TLS The TSF shall initiate communication via the trusted channel for *communication required by the Anwendungskonnektor, [for administration]*[128].

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 [17] und [19], wobei TLS 1. 2 gemäß RFC 5246 [40] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

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, and

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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 ggf. entscheiden kann, auf eine Authentisierung 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 98: Der EVG muss TLS Version 1.2 [38] unterstützen und kann zusätzlich TLS Version 1.3 [37] unterstützen (s. [19]). Der EVG unterstützt alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS, dabei werden die Anforderungen aus [19] erfüllt. Die Kryptosuiten werden für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt, sowie für die Absicherung der Administrationsschnittstellen. Der Konnektor unterstützen nicht TLS Version 1.0 und 1.1 sowie SSL.

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

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) [no additional data types][129]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS_Zert The TSF shall use [*interpretation rules*][130] 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 99: Die *interpretation rules* orientieren sich an der Konnektor-Spezifikation [17].

Anwendungshinweis 100: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [17] 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 [17]).

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

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

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

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_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 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, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*[131] 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*[132] that meet the following: *RFC 5246 [40]*.[133]

Anwendungshinweis 101: Der EVG muss TLS Version 1.2 [38] unterstützen und kann TLS Version 1.3 [37] unterstützen (s. [19]). Wird TLS 1.3 unterstützt muss die SFR FCS_CKM.1/NK.TLS um den entsprechenden Standard erweitert werden. Der EVG unterstützt alle im SFR genannten cipher suites als Algorithmen für TLS. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [42]) bzw. dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (ECDHE_RSA nach [43]) oder ECC-Signaturen (ECDHE_ECDSA mit ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch die Kurven P-256 und P-384 (FIPS PUB 186-4 [49]) und die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. RFC-5639 [48] und RFC-7027 [50])). 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 [19] beachtet. Der DH-Exponent für den Schlüsselaustausch weist eine Mindestlänge gemäß [19] auf. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange werden die gemäß [19] vorgegebenen Kurven unterstützt.

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

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

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

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

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*[134] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[135] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[136] that meet the following: *Standards FIPS 180-4 [26] and RFC 2104 [45]*[137].

Anwendungshinweis 102: FCS_COP.1/NK.TLS.HMAC wird für die Integritätssicherung innerhalb des TLS-Kanals benötigt.

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*[138] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[139] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[140] that meet

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

[135] [assignment: *cryptographic algorithm*]

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

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

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

[139] [assignment: *cryptographic algorithm*]

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

the following: *FIPS 197 [27], NIST 800-38D [42], RFC 5246 [38], RFC 8422 [41], RFC 5289 [44], specification [19]* [141].

Anwendungshinweis 103: Es gilt Anwendungshinweis 94:

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 im Standardfall von der gSMC-K bzw. SM-B durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K bzw. SM-B. In diesem Fallist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Neben der *verification of digital signatures* kann auch die *signatur creation* im EVG durchgeführt werden. Die entsprechenden privaten oder öffentlichen Schlüsselobjekte werden entweder im EVG erzeugt (FCS_CKM.1/NK.Zert) oder importiert (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* **or SM-B**[142] *storing the signing key and performing the RSA operation* [143]

c) **signature creation with help of the generated (FCS_CKM.1/NK.Zert) or imported (FDP_ITC.2/NK.TLS) signing key, performing the RSA and ECDSA operation**[144]

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

[142] Refinement: **or SM-B**

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

[144] Refinement: **c) …**

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[145] **or ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpool256r1 or NIST P-256)**[146] and cryptographic key sizes *2048 bit*[147] **or 3072 bit for RSA and 256 bit for ECDSA**[148] that meet the following: *RFC 8017 (PKCS#1) [25], FIPS PUB 180-4 [26]*[149], **Standard TR-03111 [16]**[150].

Anwendungshinweis 104: 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 oder eine eigene Zertifikatsgenerierung (siehe FCS_CKM.1/NK.Zert) bzw. ein importiertes Zertifikate/Schlüsselpaar (siehe FDP_ITC.2/NK.TLS). Im Fall der gSMC-K oder SM-B wird der dafür benötigt asymmetrische Schlüssel während der Produktion der gSMC-K oder SM-B importiert oder generiert. Es werden deshalb keine spezischen Anforderungen an die Quelle dieses Schlüssels gestellt. Für die asymmetrischen Schlüssel die im Konnektor generiert werden gilt FCS_CKM.1/NK.Zert. 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.

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 Kommunikation mit Clientsystemen zu erzeugen. Gemäß FDP_ETC.2/NK.TLS können die Zertifikate und die zugehörigen privaten Schlüssel vom Administrator exportiert werden. Keydistribution 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 sizes ***~~2048 bit~~*** **3072**[152] **bit for RSA and**

[145] [assignment: *cryptographic algorithm*]

[146] Refinement: **or ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpool256r1 or NIST P-256)**

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

[148] Refinement: **or 3072 bit for RSA and 256 bit for ECDSA**

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

[150] Refinement: **Standard TR-03111 [16]**

[151] [assignment: *Algorithm for cryptographic key generation of key pairs*]

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

256 bit for ECC with NIST P-256[153] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [24], BSI TR-03116-1 [14],*[154] **OID 1.2.840.10045.4.3.2, RFC 5639 [48], BSI TR-03111 [16].** [155]
The TSF shall

(1) create a valid X.509 [46] certificate with the generated RSA key pair and

(2) create a PKCS#12 [47] file with the created certificate and the associated private key. [156]

(3) create a valid X.509 [46] certificate with the generated ECDSA key pair[157]

Anwendungshinweis 105: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [19], 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. Die Zertifikate können für Clientsysteme oder den TOE verwendet werden, hierbei werden bei Clientzertifikate Schlüssel und Zertifikate exportiert und bei Serverzertifikaten nur die Zertifikate. Ein Export dieser Zertifikate und der zugehörigen privaten Schlüssel ist Gegenstand von FDP_ETC.2/NK.TLS. Für Clientzertifikate oder Serverzertifikate können RSA-Schlüssel nur mit 3072 bit Schlüssellänge erzeugt werden. ECC-Zertifikate mit 256 Bit Schlüssellänge können für Client- und Serverzertifikate erzeugt werden. Ergänzung: Die im PP vorgesehene Erstellung von Zertifikaten auf Basis eines RSA keys mit 2048 bit oder auf Basis von Brainpool-Kurven wurde gemäß den Vorgaben der gematik eingeschränkt.

FDP_ITC.2/NK.TLS Import of user data with security attributes

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.

153 Refinement: ~~***2048 bit***~~ **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 [48], BSI TR-03111 [16]**

156 refinement

157 Refinement: **create a valid X.509 [46] certificate with the generated ECDSA key pair**

[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*[158] 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 zugehörige private Schlüssel für den TOE durch den Administrator über die Management-Schnittstelle

(3) Die TSF importiert die Zertifikate des Objekts O_LZV_Zert_gSMCK auf Anforderung des Administrators oder automatisch wenn die existierenden Zertifikate nicht mehr länger als 180 Tage gültig sind. Die Zertifikate werden entweder aus der TI oder aus einem durch den Adminstrator bereitgestellten ZIP-Archiv importiert.]. [159]

Anwendungshinweis 106: Gemäß FMT_MOF.1/NK.TLS überlässt der Netzkonnektor die Steuerung, unter welchen Umständen der Import von Client- oder Server-Zertifikaten erfolgt, dem Anwendungskonnektor.

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]

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

[159] [assignment: *additional importation control rules*]

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*[160] 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 Serversysteme durch den Administrator über die Management-Schnittstelle]. [161]

Anwendungshinweis 107: Gemäß FMT_MOF.1/NK.TLS überlässt der Netzkonnektor die Steuerung, unter welchen Umständen der Export von Client- und Server-Zertifikaten erfolgt, dem Anwendungskonnektor.

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[162] the functions *Management of TLS-Connections*

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

[161] [assignment: *additional exportation control rules*]

[162] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

required by the Anwendungskonnektor[163]to *Anwendungskonnektor*[164].

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.**
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. **[*no additional rules*]**

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 108: 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. Only TLS 1.2 is provided.

Der Netzkonnektor nutzt die TLS-Verbindungen auch zur Absicherung der Administrationsschnittstelle. Die Verbindung wird ebenfalls durch den Anwendungskonnktor gemanagt.

Erläuterung: Im Schutzprofil für den Konnektor werden diese Regeln durch verschiedene SFRs für den Anwendungskonnektor konkretisiert.

Anwendungshinweis 109: Es wurden keine SFRs aus dem Schutzprofil des Gesamtkonnektors [11] bezüglich Managment der TLS-Verbindungen übernommen. Das Managment erfolgt durch den Anwendungskonnektor.

[163] [assignment:*list of functions*]

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

[165] refinement

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.

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 komplett und unverändert aus NK-PP [12] übernommen, sodass alle hier dargestellten Informationen in sich konsistent sind.

6.4.1. Abbildung der EVG-Ziele auf Sicherheitsanforderungen

Tabelle 7 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_Protokoll	O.NK_Zeitdienst	O.NK_Update	O.NK_Admin_Auth	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	
FMT_MTD.1/NK				X											
FIA_UID.1/NK.SMR				X											
FIA_UAU.1/NK.SMR				X				X							
FTP_TRP.1/NK.Admin	X			X				X							
FMT_SMF.1/NK	X			X									X	X	
FMT_MSA.1/NK.PF				X									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				
FCS_CKM.1/NK		X	X						X		X	X			
FCS_CKM.2/NK.IKE									X		X	X			

Sicherheitsanforderung an den EVG	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_Admin_Auth	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.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								
FDP_ITC.1/NK.Update							X								
FDP_UIT.1/NK.Update							X								

Tabelle 7: 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 8 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 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

[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

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 6.2.8)
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 Gültigkeitsprüfung von Zertifikaten	FCS_CKM.1/NK.Zert FCS_CKM.4/NK FDP_ITC.2/NK.TLS FTP_TRP.1/NK.Admin FDP_ETC.2/NK.TLS 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.	
	sichere kryptographische Algorithmen und Protokolle	FCS_CKM.1/NK.TLS FCS_COP.1/NK.TLS.HMAC

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
		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 [19]*“ 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.Schutzund als Oberbegriff für die weiteren Teilaspekte zu verstehen. „*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,*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	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
	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*	

<table>
<tr><th>EVG-Ziel</th><th>Aspekt des Ziels</th><th>SFR, SAR
(vgl. Abschnitt 6.2 oder 6.2.8)</th></tr>
<tr><td></td><td colspan="2">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.</td></tr>
<tr><td rowspan="2">O.NK.Admin_EVG</td><td>rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen
Identifikation / Autorisierung des Administrators
sicherer Pfad
Beschränkung der Administration der Firewall-Regeln</td><td>FMT_MTD.1/NK
FMT_SMR.1./NK
FMT_SMF.1/NK
FIA_UID.1/NK.SMR
FIA_UAU.1/NK.SMR

FTP_TRP.1/NK.Admin
FMT_MSA.1/NK.PF</td></tr>
<tr><td colspan="2">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. Die dabei anzuwendenden Regeln wurden in FIA_UAU.1/NK.SMR 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 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).</td></tr>
</table>

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	„*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.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: „*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	Software Update	FDP_ACC.1/NK.Update FDP_ACC.1/NK.Update FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
	Begründung: Das Sicherheitsziel O.NK.Update „Software Update“ fordert vom EVG die Aktualisierung von Software-Komponenten sowie deren Prüfung auf Integrität. FDP_ACC.1/NK.Update führt die Update-SFP für den Software-Update ein und FDP_ACC.1/NK.Update definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_ITC.1/NK.Update fordert die Fähigkeit des EVG zum Import der Software-Komponenten von ausserhalb des EVG und FDP_UIT.1/NK.Update fordert die Prüfung der Integrität dieser Daten vor dem Update.	
O.NK.Admin_Auth	Authentisierung des Administrators	FTP_TRP.1/NK.Admin

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
		FIA_UAU.1/NK.SMR FTP_ITC.1/NK.TLS
	Begründung: FTP_TRP.1/NK.Admin fordert einen sicheren Kommunikationskanal zwischen EVG und Administrator. FTP_ITC.1/NK.TLS fordert dazu einen TLS-Kanal für lokale und entfernte Administrierung. Erst nach erfolgreicher Authentisierung können adminstrative Funktionen aufgerufen werden (FIA_UAU.1/NK.SMR).	
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 Authentifizierung („ … 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 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.*“	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	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 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*.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	„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
	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)	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	(RFC 4303 (ESP), [31]) erfolgt. 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], [32]). 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: „*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.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	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): „*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:	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.2.8)
	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 8: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 110: H
inweis zu O.NK.VPN_Integrität: Zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash wird eine Hashfunktion verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruht, es sind daher keine entsprechenden 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 9 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 9: 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

Die Definition von Erweiterungen ist durch das PP [12] vorgegeben. Dieses Security Target definiert keine weiteren Erweiterungen.

6.6. Erklärung für die gewählte EAL-Stufe

Die EAL Stufe ist durch das PP [12] vorgegeben. Dieses Security Target übernimmt die EAL Stufe ohne weitere Augmentierungen.

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 (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, Software Update.
- Kryptografische Basisdienste
- TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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 (Bei Verbindungen zum *VPN-Konzentrator der Telematikinfrastruktur* siehe FTP_ITC.1/NK.VPN_TI und bei Verbindungen zum *Sicheren Internet Service (SIS)* siehe FTP_ITC.1/NK.VPN_SIS). Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei wird IKEv2 unterstützt.

Informationsflusskontrolle

Regelbasiert nutzen alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel. Nur Informationsflüsse, die vom Konnektor initiiert wurden sowie Informationsflüsse von Clientsystemen in Bestandsnetze dürfen den VPN-Tunnel in die Telematikinfrastruktur benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale Telematikinfrastruktur-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen

Netzen der Leistungserbringer betreffen, nutzen den VPN-Tunnel zum zum Sicheren Internet Service.

Diese Aspekte ergeben sich aus der Betrachtung der VPN-Kanäle. Sie werden 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 Abschnitt 6.2.2) zugeordnet.

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. Dies wird durch die Administratordokumentation (siehe das Refinement zu AGD_OPE.1 in Abschnitt 6.2.8) sichergestellt.

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 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

Der EVG führt in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Siehe auch Sicherheitsdienst Zeitdienst (siehe FPT_STM.1/NK).

Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand an der Außenhaut des Konnektors anzeigt, um die Anforderung gemäß Konnektor-Spezifikation [17], Abschnitt 3.3 *Betriebszustand* umzusetzen, siehe LS9 und PS5 in Kapitel 1.3.3 sowie die Anforderungen an die Konnektor Hardware in Kapitel 1.3.6.

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 (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). Es wird bei Programmstart eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) durch Verifikation von Signaturen durchgeführt (unter Verwendung von RSA 2048 und SHA 256, siehe FCS_COP.1/NK.Auth). Dazu verifiziert der UEFI BIOS die Signatur des Bootloaders. Dieser verifiziert die Signatur über den Betriebssystemkernel und die Inital RAM Disc. In der Inital RAM Disc ist das Root Dateisystem enthalten. Die öffentlichen Prüfschlüssel zur Verifikation der Integrität sind jeweils in den Prüfenden Komponenten hinterlegt (intialer Boot Schlüssel des UEFI im Secure ROM, Boot Schlüssel des Bootloaders im Drive Security Sector). Die Selbsttest-Funktion (Secure Boot) kann nicht deaktiviert bzw. manipuliert werden. Die jeweiligen Prüfroutinen werden durch die sichere Bootchain, angefangen mit dem UEFI BIOS abgesichert.

Damit 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 TOE. Dieser ist durch die Prüfung der Integrität ebenfalls vor Manipulationen abgesichert. Der Benutzer kann die Selbsttests durch Neustart des EVGs selbst anstoßen. Schlägt die Prüfung der Integrität fehl, so wird ein Neustart des EVG durchgeführt. Dies führt dann bei manipulierten Komponenten zu einem „Endless Loop“

Im Falle einer Software-Aktualisierung wird dieselbe Bootchain abgelaufen, aber vom Bootloader das neue SW Image geprüft und geladen. Schlägt die Prüfung der Integrität fehl, so wird ein Neustart des EVG durchgeführt und dann das ursprüngliche SW Image geladen.

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 4: Sekundäre Werte in Abschnitt 3.1.2).

Der private Authentisierungsschlüssel für das VPN wird bereits durch das 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 [17], 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 FIA_UAU.1/NK.SMR), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1/NK). Die Authentisierung erfolgt dabei durch den Netzkonnektor selbst, siehe O.NK.Admin_Auth.

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 bzw. FTP_ITC.1/NK.TLS).

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

Signierte Update-Pakete werden importiert (FDP_ITC.1/NK.Update) und im Datenspeicher des EVG abgelegt. Sobald ein Update-Paket zur Verfügung steht signalisiert der TOE das ein Software Update zur Verfügung steht. Der Administrator kann die Version des Update-Paketes

prüfen und den Updateprozess anstossen (FDP_ACC.1/NK.Update. Automatische Installation von Software Updates wird vom EVG nicht unterstützt (FDP_ACF.1/NK.Update).

Im Falle einer Software-Aktualisierung wird der EVG neu gestartet und dieselbe Bootchain wie in der Sicherheitsfunktion „Selbstschutz“ beschrieben abgelaufen, aber vom Bootloader wird das neue Update-Paket auf Integrität geprüft und bei erfolgreicher Prüfung geladen. Das alte Image wird vom EVG verworfen. Schlägt die Prüfung der Integrität fehl, so wird das Update-Paket verworfen und ein Neustart des EVG durchgeführt mit dem das ursprüngliche SW Image geladen wird. Durch die Prüfung des Update-Pakets analog zum regulären Boot Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können (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]“ [19] die im Folgenden aufgelistete kryptographischen Primitive.

- Hash-Berechnung, siehe FCS_COP.1/NK.Hash
- HMAC-Berechnung, siehe FCS_COP.1/NK.HMAC
- Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256 und RSA bzw. ECDSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen, siehe FCS_COP.1/NK.Auth
- Ver- und Entschlüsselung mittels symmetrischer Algorithmen (AES im CBC Modus mit 256bit Schlüssellänge oder AES im GCM Modus mit 128bit und 256bit Schlüssellänge) zur Unterstützung der Absicherung des IPsec-Tunnels, siehe FCS_COP.1/NK.ESP
- VPN Kommunikationsprotokoll zur Absicherung des IPsec-Tunnel, siehe FCS_COP.1/NK.IPsec
- Erzeugung von Schlüsseln für die VPN-Kanäle mit hoher Qualität 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)
- Schlüsselaustausch (IPsec IKEv2) zum Aufbau von VPN-Tunnel, siehe FCS_CKM.2/NK.IKE
- Schlüsselvernichtung für nicht mehr benötigte Schlüssel durch Überschreiben mit Nullen, siehe FCS_CKM.4/NK

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 dem Anwendungskonnektor die Dienste zum Aufbau eines TLS Kanals zur Verfügung FTP_ITC.1/NK.TLS. TLS wird auch zur Absicherung der Administrator-Schnittstelle verwendet. Dabei werden nur die folgenden Cipher Suites unterstützt:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
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, and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Der Netzkonnektor implementiert entsprechend die im Folgenden aufgelisteten kryptographischen Primitiven für TLS.

- HMAC-Berechnung, siehe FCS_COP.1/NK.TLS.HMAC
- Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256, ECDSA und RSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen, siehe FCS_COP.1/NK.TLS.Auth
- Ver- und Entschlüsselung mittels symmetrischer Algorithmen (AES im CBC und GCM Modus mit 128 bit und 256bit Schlüssellänge) zur Unterstützung der Absicherung des TLS-Kanals, siehe FCS_COP.1/NK.TLS.AES
- Erzeugung von Schlüsseln für die TLS-Kanäle mit hoher Qualität für alle oben benannten kryptographischen Algorithmen (FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.Auth, FCS_COP.1/NK.TLS.AES), siehe FCS_CKM.1/NK.TLS
- Schlüsselvernichtung für nicht mehr benötigte Schlüssel durch Überschreiben mit Nullen, siehe FCS_CKM.4/NK

Die kryptographischen Basisdienste für TLS (z.B. HMAC-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 TLS Kanals).

Zertifikate die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen werden vom Netzkonnektor entsprechend den Vorgaben aus FPT_TDC.1/NK.TLS.Zert interpretiert. Der EVG prüft insbesondere, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist enthalten ist.

Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen werden X.509 Zertifikate verwendet. Entsprechende Zertifikate für die Kommunikation mit Clientsystemen können vom EVG erzeugt werden (FCS_CKM.1/NK.Zert). Der EVG bietet dem Administartor eine sichere Schnittstelle zum exportieren dieser X.509 Zertifikate für

Clientsysteme und die zugehörigen privaten Schlüssel (FDP_ETC.2/NK.TLS). Bei Zertifikaten für Serversysteme werden die zugehörigen privaten Schlüssel nicht exportiert. Zertifikate für die Kommunikation mit Clientsystemen 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 ebenfalls nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.

Die TLS-Verbindungen werden vom Anwendungskonnektor gemanagt und je nach Anwendungsfall eingerichtet (FMT_MOF.1/NK.TLS, FMT_SMR.1./NK).

7.2. Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen

Tabelle 10 im folgenden Abschnitt 7.2.1 stellt die Abbildung der Sicherheitfunktionlität 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		
FIA_UAU.1/NK.SMR						X		
FTP_TRP.1/NK.Admin						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**
FMT_SMF.1/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	
FCS_CKM.1/NK							X	
FCS_CKM.2/NK.IKE							X	
FCS_CKM.4/NK							X	
FDP_ACC.1/NK.Update						X		
FDP_ACF.1/NK.Update						X		
FDP_ITC.1/NK.Update						X		
FDP_UIT.1/NK.Update						X		
FTP_ITC.1/NK.TLS								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

Tabelle 10: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen

7.2.2. Erfüllung der funktionalen Sicherheitsanforderungen

Wie aus der Tabelle 10 ersichtlich, wird jede Sicherheitsanforderung gemäß Kapitel 6.2 durch die Sichrheitsfunktionen in Kapitel 7.1 umgesetzt. Die Beschreibung der Sicherheitsfunktionen in den Kapiteln 7.1.1-7.1.7 nutzen direkte Referenzen auf die entsprechenden implementierten Sicherheitsfunktionen in Kapiteln 6.2.1-6.2.7. Die Sicherheitsfunktionen sind dabei direkt aus der Unterteilung der Sicherheitsfunktionen im NK-PP [12] 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 111: 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 [29]
AK	Anwendungskonnektor: Der Teil des Gesamtkonnektors, der nicht Netzkonnektor ist, wird als Anwendungskonnektor bezeichnet.
AK-PP	Schutzprofil 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 [30] bzw. zukünftig RFC 4303 [31]; für die jeweils zu verwendenden Standards siehe die Konnektorspezifikation [17]
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
IAG	Internetzugangspunkt des Leistungserbringers
IKE	Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 [32]
IP	Internet Protocol
IPsec	IP Security, vgl. RFC 2401 bzw. RFC 4301 [28]
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 sowie SAK)
NK-PP	Schutzprofil für den Netzkonnektor
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	Signaturanwendungskomponente (hier stets: Signaturanwendungskomponente des Konnektors), einer der Hauptfunktionsblöcke des Konnektors (siehe auch NK und Ablaufkontrolle)
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
SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Sicherer Internet Service: Ein Internet-Zugangspunkt, der die damit verbundenen lokalen Netze und Systeme gegen Angriffe aus dem Internet schützt.
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 [21] erfüllt, wird es als SMC-K bezeichnet
SM-KT	Sicherheitsmodul für das Kartenterminal
SM-SAK	Sicherheitsmodul (für die) Signaturanwendungskomponente (SAK) des Konnektors Bezeichnung für die Anwendung auf dem Sicherheitsmodul SM-K (oder einem der Sicherheitsmodule SM-K) des Einbox-Konnektors, welches das von der SAK benötigte Schlüsselmaterial speichert.

Abkürzung	Bedeutung
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-Plattform verwendet; beispielsweise kann das Internet als Transportmedium für ein VPN genutzt werden

Abkürzung	Bedeutung
X.509	Standard der ITU-T (International Telecommunication Union) für Public Key Infrastrukturen und insbesondere für den Aufbau von Zertifikaten
xSAK	extended SAK (Signaturanwendungskomponente)
xTV	Extended Trusted Viewer, sichere Anzeigekomponente der SAK gemäß SigG/SigV

Tabelle 11: 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, SAK) 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.
CRL Download Server	Ein von der PKI der TI bereitgestellter Downloadpunkt im Internet, von dem der Konnektor die aktuelle CRL erhalten kann.
hash&URL server	Der hash&URL-Server ist ein http-Server, der die zur gegenseitigen Authentifizierung von Konnektoren und VPN-Konzentratoren genutzten Zertifikate gemäß [RFC7296] zum Download bereitstellt.
Registration server of the VPN network provider	Der Registrierungsserver ist ein http-Server, welcher Anfragen des Konnektors zur Registrierung des Konnektors durch den berechtigten Teilnehmer beim Anbieter entgegennimmt und bearbeitet.
remote management server	Management-Gegenstelle für das Remote-Management des Konnektors (sofern dieses angeboten wird).
Service modules (Fachmodule)	Fachmodule im Konnektor, die die Anwendungslogik der Fachanwendungen im Konnektor umsetzen und (Sicherheits-)Funktionen des Konnektors nutzen

Begriff	Bedeutung
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
TI Services	zentrale Dienste und Fachdienste der Telematikinfrastruktur
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
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*

Begriff	Bedeutung
	Kommunikationskanal in die Telematikinfrastruktur aufzubauen. […]“

Tabelle 12: Glossar

8.4. Abbildungsverzeichnis

Abbildung 1: Funktionsblöcke des Konnektors 13
Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung) 16
Abbildung 3: Konnektor: externe, physische und logische Schnittstellen 20
Abbildung 4: Konnektor Architekturkonzept (schematisch) 21
Abbildung 5: Konnektor Architektur Komponentenansicht (schematisch) 21
Abbildung 6: Netzkonnektor Komponenten 22
Abbildung 7: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade 38

8.5. Tabellenverzeichnis

Tabelle 1: Komponenten der Einbox-Lösung 11
Tabelle 2: Mindestanforderungen für Komponenten der Einbox-Konnektor Hardware 27
Tabelle 3: Primäre Werte 32
Tabelle 4: Sekundäre Werte 34
Tabelle 5: Kurzbezeichner der Bedrohungen 38
Tabelle 6: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen 63
Tabelle 7: Abbildung der EVG-Ziele auf Sicherheitsanforderungen 122
Tabelle 8: Abbildung der EVG-Ziele auf Anforderungen 133
Tabelle 9: Erfüllung der Abhängigkeiten der augmentierten Komponenten 134
Tabelle 10: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen 142
Tabelle 11: Abkürzungsverzeichnis 148
Tabelle 12: Glossar 150

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 1b G. v. 20.12.2022 BGBl. I S. 2793)

8.6.3. Schutzprofile und Technische Richtlinien

[10] Common Criteria Protection Profile: Card Operating System (PP COS G2), BSI-CC-PP-0082-V4-2019, 10.07.2019 und jede darauf angewandte Maintenance und Re-Zertifizierung, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[12] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.7, 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 2023-01

[14] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Bundesamt für Sicherheit in der Informationstechnik, Version 3.20, 21.09.2018, Technische Arbeitsgruppe TR-03116-1

[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, Bundesamt für Sicherheit in der Informationstechnik

[16] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

8.6.4. Spezifikationen

[17] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon]: Version 5.20.0, 05.05.2023, gematik GmbH,

[18] Elektronische Gesundheitskarte und Telematikinfrastruktur: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], GmbH, Version 1.23.0, 16.12.2022

[19] Elektronische Gesundheitskarte und Telematikinfrastruktur- Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik GmbH, Version 2.27.0, 14.04.2023

[20] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation des Card Operating System (COS) Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik GmbH

[21] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation der gSMC-K / Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.14.0, 12.05.2022, gematik GmbH

[22] Elektronische Gesundheitskarte und Telematikinfrastruktur. Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM]. Version 1.14.0, Stand 26.06.2020, gematik GmbH

8.6.5. Standards

[23] D. Mills, U.Delaware, J. Martin, J.Burbank, W.Kasch: Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010, RFC 5905 (NTPv4), http://www.ietf.org/rfc/rfc5905.txt

[24] 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, http://www.rfc-editor.org/rfc/rfc4055.txt

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

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

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

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

[29] S. Kent: IP Authentication Header, December 2005, RFC 4302 (AH), http://www.ietf.org/rfc/rfc4302.txt

[30] S. Kent, R. Atkinson: IP Encapsulating Security Payload (ESP), November 1998, RFC 2406 (ESP), http://www.ietf.org/rfc/rfc2406.txt

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

[32] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, RFC 7296 (IKEv2), http://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, http://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, http://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, http://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, http://www.rfc-editor.org/rfc/rfc3526.txt

[37] R. Droms: Dynamic Host Configuration Protocol. March 1997, RFC 2131, http://www.ietf.org/rfc/rfc2131.txt

[38] S. Alexandwer, R. Droms: DHCP Options and BOOTP Vendor Extensions. March 1997, RFC 2132, http://www.ietf.org/rfc/rfc2132.txt

[39] RFC 8446 (August 2018): The Transport Layer Security (TLS) Protocol, Version 1.3

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

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

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

[43] RFC 8422 (August 2018): Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), Version 1.2 and Earlier

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

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

[46] 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

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

[48] RFC 5639 (March 2020): Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, https://tools.ietf.org/html/rfc5639

[49] NIST: FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[50] RFC 7027 (October 2013): Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), http://www.ietf.org/rfc/rfc7027.txt

[51] J. Viega, D. McGrew: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). June 2005, RFC 4106, http://www.rfc-editor.org/rfc/rfc4106.txt

8.6.6. Dokumentation

[52] secunet konnektor, Bedienhandbuch, Für Administratoren und Benutzer, Version 6.8.5, Produkttypversion: 5.61.0-0 (PTV5 Wartungsrelease 4), Firmwareversion: 5.70.4, 10.04.2025, secunet Security Networks AG

[53] secunet konnektor, Modularer Konnektor Version 2.0.0, Hinweise und Prüfpunkte für Endnutzer, Version 2.0, Secunet Security Networks AG

[54] secunet konnektor, Modularer Konnektor, Konnektor Management API-Dokumentation, Version 5.1.1, eHealth Experts GmbH, 7.10.2024