Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Schutzprofil (Protection Profile)

Schutzprofil 1:
Anforderungen an den Netzkonnektor

BSI-CC-PP-0097

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungsverlauf

Version	Datum	Änderungen
0.9.0	28.02.2017	Erstversion basierend auf BSI-CC-PP-0047, Version 3.2.2 Anpassungen: Aufnahme der Anforderungen zu TLS-Kanälen, allgemeine Anpassungen zur Konsistenz mit Konnektor-PP.
1.0	21.03.2017	Version zur Evaluierung
1.1	17.07.2017	Einarbeitung von Herstellerkommentaren
1.2	26.07.2017	• Entfernung DNSSEC • Entfernung von RFC 5996, Ablösung durch RFC 7296 • aktuellere Alternativreferenzen zu [17] und [12] eingefügt
1.3	31.08.2017	Einarbeitung der Kommentare der Prüfstelle
1.4	27.09.2017	Finale Version
1.5	27.04.2018	Anwendungshinweise zur Nutzung von AES-NI Fehlerkorrektur in FDP_IFF.1.2/NK.PF
1.6	07.10.2019	Anpassungen der Forderungen zu Versionen des TLS Protokolls
1.6.4	17.03.2020	Einarbeitung der Kommentare der Prüfstelle

Editorieller Hinweis:

Um die Konformität des Konnektors zum Schutzprofil BSI-CC-PP-0097 im Sinne einer sicheren Umsetzung der Sicherheitsanforderungen zu gewährleisten, wird dem Hersteller dringend empfohlen, seine Umsetzung der Sicherheitsfunktionalität frühzeitig mit der Zertifizierungsstelle abzustimmen. Hierdurch bekommt der Hersteller rechtzeitig ein Feedback, ob die getroffenen Maßnahmen zeitgemäß sind. Es wird explizit begrüßt, wenn bei dieser Abstimmung die mit der CC-Evaluierung beauftragte Prüfstelle mit dabei ist. Dem Hersteller muss aber bewusst sein, dass die Ergebnisse der Abstimmung nur unverbindlich sein können, da erst die CC-Evaluierung des Produkts nachweist, dass die konkrete Umsetzung der Sicherheitsfunktionalitäten gemäß gewählter AVA_VAN-Stufe sicher ist.

Inhaltsverzeichnis

1. PP-Einführung

1.1. PP-Referenz

Titel: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor

Version des Dokuments: 1.6.4

Datum des Dokuments: 17.03.2020

Allgemeiner Status: Version für den Konnektor der Produkttypversion 3 (PTV3) und 4 (PTV4)

Registrierung: BSI-CC-PP-0097

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

Auftraggeber und Sponsor: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Editor: Initiale Erstellung sowie Pflege
(BSI-CC-PP-0047, 2005-2009, Versionen bis 1.05 und ab 1.90 aufwärts)
Prüfstelle IT-Sicherheit der T-Systems GEI GmbH

Überarbeitung des Schutzprofils (zur BSI-CC-PP-0097 Version 1.4):
Holger Ebel (http://www.its-ebel.com) und Prüfstelle der SRC Security Research and Consulting GmbH

Stichwörter: Konnektor, Netzkonnektor, eHealth, Telematikinfrastruktur, dezentrale Komponente

Dieses Schutzprofil wurde konform zu den folgendenden 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 7.7 (insbesondere Abschnitt 7.7.4) aufgeführt sind; allen voran die Konnektorspezifikation:

[15] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec_Kon], gematik GmbH, PTV3: Version 5.4.0, 26.10.2018, zuzüglich der Errata 1 bis 6 für den PTV3 Konnektor, PTV4: Version 5.9.0, 02.03.2020

1.2. PP-Übersicht

Dieses Schutzprofil beschreibt den Schutzbedarf für einen Netzkonnektor als Bestandteil des Konnektors im Gesundheitswesen gemäß Spezifikation [15]. Zu den gesetzlichen Grundlagen siehe Abschnitt 7.1 *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. 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 ist konform zum Schutzprofil BSI-CC-PP-0082 [10] zertifiziert, das Objektsystem der gSMC-K ist nach der Technischen Richtlinie TR-03144 [14] zertifiziert.

Der EVG des vorliegenden PP schließt die gSMC-K nicht ein, um eine Evaluierung und Zertifizierung des Netzkonnektors ohne zertifizierte gSMC-K zu ermöglichen. Es steht dem Autor der zu dem vorliegenden Schutzprofil konformen Sicherheitsvorgaben frei, den EVG um die gSMC-K und die für den Netzkonnektor benötigte Sicherheitsfunktionalität zu erweitern. Dann gehen die relevanten Sicherheitsziele der Einsatzumgebung, wie OE.NK.gSMC-K, OE.NK.KeyStorage und ggf. OE.NK.RNG auf Sicherheitsziele des EVG der Sicherheitsvorgaben über.

Die Konnektorspezifikation [15] 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.

Dieses Schutzprofil beschreibt nicht die verschiedenen Möglichkeiten Umgebungsziele zu erfüllen. Insbesondere werden keine Aussagen dazu getroffen,

- wie der im Umgebungsziel OE.NK.phys_Schutz geforderte physische Schutz realisiert werden kann,
- auf welche Weise ein Sicherheitsmodul gSMC-K wie von OE.NK.gSMC-K gefordert sicher mit dem Netzkonnektor verbunden werden kann, und
- wie Denial of Service Angriffe aus dem WAN oder aus dem LAN verhindert werden können (siehe auch OE.NK.kein_DoS).

1.2.2. Terminologie

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

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

Audit-Daten vs. Logging: Der Begriff Audit-Daten wird in diesem Schutzprofil im Sinne der Common Criteria verwendet. Im Sinne der Common Criteria bezeichnet dieser Begriff ganz allgemein Anforderungen aus der Klasse FAU (Security Audit) aus Common Criteria Teil 2 [2], die im Gesundheitswesen eher mit „Logging“ bezeichnet würden. Dieses Schutzprofil

---

[1] Ein Glossar der wichtigsten Begriffe befindet sich im Anhang in Abschnitt 7.3. 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 [15] 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.

verwendet ebenfalls den Begriff „Logging“, wo dies möglich ist, nutzt aber auch den Begriff „Audit“, wenn z. B. funktionale Anforderungen aus den Common Criteria zitiert werden. Die Funktionalität, die üblicherweise unter dem Begriff „Audit“ verstanden wird, wird hier durch O.NK.Protokoll gefordert.

1.3. EVG-Beschreibung

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

1.3.1. EVG-Typ

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

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

Der Konnektor erbringt Sicherheitsleistungen in vier wesentlichen Funktionsblöcken. Die Sicherheitsfunktionalität einer Firewall, eines VPN-Clients, und von Servern für Zeitdienst, Namensdienst und DHCP-Dienst werden durch den Bestandteil Netzkonnektor (EVG) erbracht, ebenso die Basisdienste zum Aufbau von TLS-Kanälen. Die Sicherheitsfunktionalität einer Signaturanwendung, eines Kryptomoduls für die Verschlüsselung und für die Initiierung der gesicherten Kommunikation zwischen dem Konnektor und dem Clientsystem, zwischen Fachmodulen und Fachdiensten sowie zwischen Servern und dem Kartenterminaldienst, dem Chipkartendienst, werden durch den Anwendungskonnektor erbracht. Das Sicherheitsmodul gSMC-K stellt interne Sicherheitsfunktionalität zur Speicherung von Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit.

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.

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

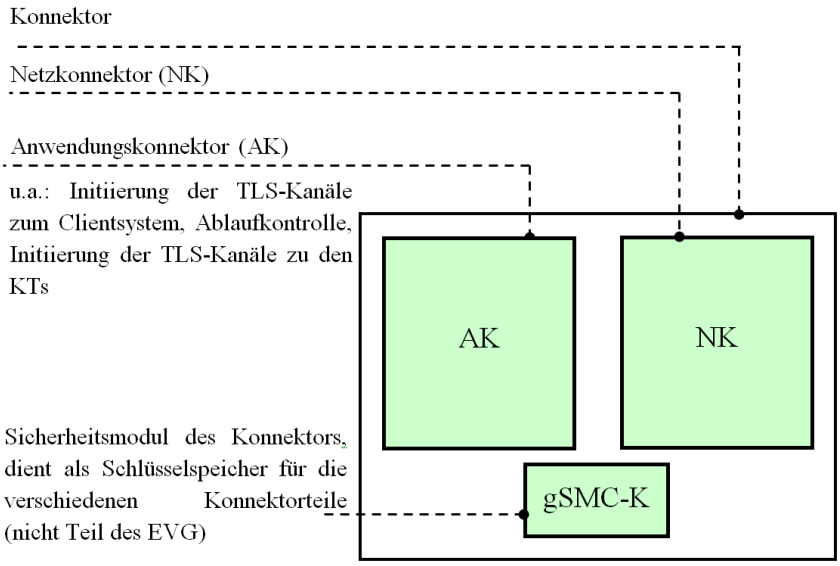

Abbildung 1: Funktionsblöcke des Konnektors

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[3] 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: Die in diesem Kapitel genannten Anforderungen beziehen sich auf den Konnektor als Ganzes. Die Anforderungen für den Netzkonnektor, der Gegenstand dieses Schutzprofils ist, werden im Verlauf dieses Schutzprofils präzisiert.

Anwendungshinweis 2: **Mechanismen zum Integritätsschutz:** Der Konnektor muss keinen Schutz vor Hardware-Manipulationen bieten (siehe Annahme A.NK.phys_Schutz in Abschnitt 3.5), wohl aber Mechanismen zum Integritätsschutz seiner Software implementieren. Siehe auch die Anforderung FPT_TST.1/NK und Anwendungshinweis 77.

1.3.2. Einsatzumgebung des Konnektors

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

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

Anwendungshinweis 3: In diesem Schutzprofil wird von der Standard-Situation „**Einbox-Lösung**“ ausgegangen. Dieser Begriff bedeutet, dass

[3] Diese Authentisierung ist nicht Gegenstand des Schutzprofils.

- 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 ST-Autor soll in konsistenter Weise beschreiben, welchen Bedrohungen die Verbindungen zwischen Anwendungskonnektor, Netzkonnektor und gSMC-K ausgesetzt sind, welche Annahmen an die Einsatzumgebung gelten und welche Funktionalität genau der EVG im Hinblick auf sichere Kanäle bietet. – Siehe auch Abschnitt 7.6.15.

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

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

Der ST-Autor soll beschreiben, welche Bereiche durch die Einsatzumgebung zu schützen sind. Dazu kann er Abbildung 2 verändern oder eine vergleichbare Skizze erstellen.

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

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

In der folgenden Abbildung 2 bedeuten die Abkürzungen (siehe auch Kapitel 7.2):

- NK: Netzkonnektor
- EVG: Evaluierungsgegenstand (TOE)
- 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, Apotheken-verwaltungssystem, Krankenhaus-Informationssystem).
- PVS: Praxis-Verwaltungssystem. Dieser Ausdruck steht stellvertretend auch für Apotheken-Verwaltungssysteme (AVS) oder Krankenhaus-Informationssysteme (KIS). Er bezeichnet den Softwareanteil auf dem Clientsystem. Das Betriebssystem des Clientsystems ist in den folgenden Abbildungen nicht dargestellt.
- eGK: elektronische Gesundheitskarte
- HBA: Heilberufsausweis
- SM-B: Security Module Card Typ B oder HSM-B, Träger der kryptographischen Identität der Institution des Leistungserbringers
- gSMC-K: Sicherheitsmodul für den Konnektor
- SIS: Sicherer Internet Service
- TI Telematikinfrastruktur-Plattform
- VSDM: Versichertenstammdatenmanagement
- VSDD: Versichertenstammdatendienst

Anwendungshinweis 4: Der **WAN-Router** kann mit dem Netzkonnektor in einem gemeinsamen Gehäuse integriert sein, ist aber nicht notwendigerweise Teil des Netzkonnektors im Sinne dieses Schutzprofils. Der WAN-Router muss auch bei Integration in einem Gehäuse, auf einer Platine oder in einer Baugruppe mit dem (Netz-) Konnektor, keinen Teil des Konnektors darstellen, da er keine Sicherheitsfunktionalität im Sinne des Schutzprofilsbereitstellt. Vielmehr handelt es sich dann um ein multifunktionales Gerät, bei dem ein Konnektor (gemäß den Konnektor-Schutzprofilen) und ein WAN-Router im selben Gehäuse integriert wurden. Es ist zulässig, dass ein integrierter WAN-Router im ST physisch als nicht zum EVG gehörig abgegrenzt wird. WAN-Router-Funktionalität kann z. B. mit einem DSL-Modem integriert werden. In jedem Fall besitzt der WAN-Router keine Sicherheitsfunktionalität im Sinne des Schutzprofils und somit keine zu evaluierende Sicherheitsfunktionalität. Der ST-Autor soll eine exakte physische und logische Abgrenzung des EVG vornehmen und beschreiben, ob und ggf. welche Funktionalitäten der EVG zusätzlich zu den Sicherheitsfunktionalitäten bietet.

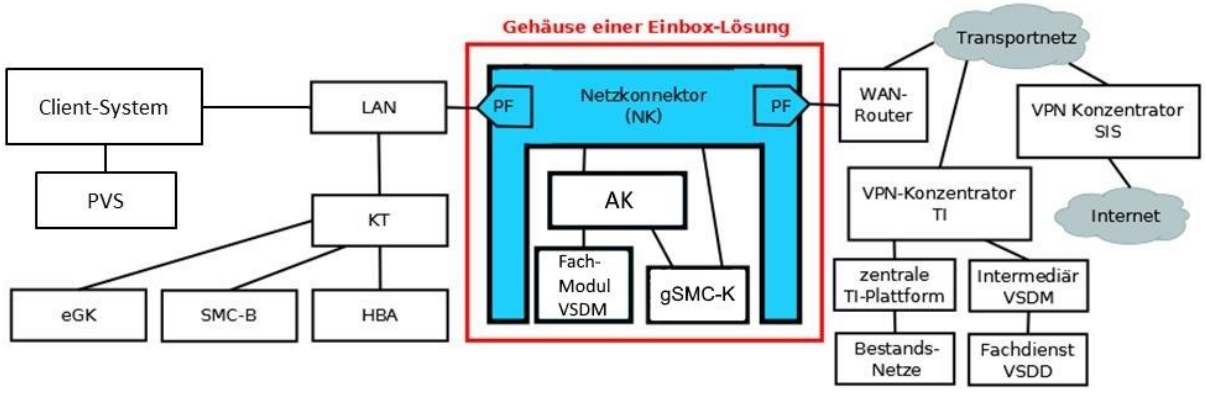

Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung)

Im betrachteten Fall, dass der Konnektor als Einbox-Lösung ausgestaltet ist, wird vom Netzkonnektor gefordert, dass er den Anwendungskonnektor vor Angriffen aus dem LAN schützt. Auf eine zusätzliche Firewall außerhalb des Einboxkonnektors zum Schutz des Anwendungskonnektors vor Angriffen aus dem LAN kann dann verzichtet werden.

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

Anwendungshinweis 5: Der ST-Autor muss im Security Target die Einsatzumgebung eindeutig beschreiben. Er sollte dazu eine Skizze erstellen, vergleichbar zu Abbildung 2. Die Skizze muss geeignet sein, die physischen und logischen Schnittstellen zwischen dem EVG und seiner IT-Umgebung zu erkennen. Abhängig von der konkreten Ausprägung des Produkts ist die Beschreibung der Schnittstellen in Abschnitt 1.3.3 geeignet anzupassen.

Anwendungshinweis 6: Dieses Schutzprofil modelliert Sicherheitsanforderungen an einen Einbox-Konnektor (Einboxlösung). Dennoch wird in den Anwendungshinweisen in Abschnitt 7.6.3 eine verallgemeinernde Skizze zur Einsatzumgebung des Konnektors im Fall einer Mehrkomponenten-Lösung dargestellt (vgl. Abbildung 4).

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: Dies kann beispielsweise dadurch erreicht werden, dass von den Clientsystemen außer der Verbindung über den Netzkonnektor keine weiteren Verbindungen in potentiell unsichere Netze existieren. Der ST-Autor soll beschreiben, ob und ggf. welche speziellen Annahmen getroffen werden.

Anwendungshinweis 8: **Spezielle Einsatzumgebungen:** Falls für ein Produkt der Einsatz in speziellen Umgebungen (z. B. Krankenhaus, mobiler Einsatz) geplant ist, soll dies im Security Target thematisiert werden. Aus den veränderten Einsatzbedingungen können sich zusätzliche spezifische Anforderungen ergeben.

Die Konnektor-Spezifikation sieht unterschiedliche netzseitige Einsatzszenarien vor (siehe Kapitel 2.7 und Anhang K in [15]). Der Konnektor bietet dazu Konfigurationsparameter, die je nach Einsatzszenario konfiguriert werden müssen. Dadurch wird die Verwendung des SIS abhängig von dieser Konfiguration, zum Zugriff auf das Internet kann auch ein bereits vorhandenes Gateway benutzt werden. Für dieses Schutzprofil hat dieser Fall insofern keinen Einfluss, da die Schutzmechanismen des SIS nun durch das vorhandene Gateway zu erbringen sind (OSP.NK.SIS).

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 9: Der ST-Autor soll die Beschreibung der physischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Netzkonnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern und zu begründen.

Der EVG besitzt folgende physische Schnittstellen:

PS1 Im Fall Mehrboxlösung: Eine physische Schnittstelle zum Anwendungskonnektor.

PS2 Eine Schnittstelle zum LAN bzw. zum Clientsystem.

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

PS3 Eine Schnittstelle zu Datennetzen (WAN), welche als Transportnetz für den Zugang zur Telematikinfrastruktur und ggf. zum Internet dienen. Es wird angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und Verbindungen mit ihnen nicht notwendigerweise verschlüsselt sind.[4]

Anwendungshinweis 10: Im Fall der Einboxlösung ist die Identifizierung einer physischen Schnittstelle zwischen Netzkonnektor und dem Annwendungskonnektor nicht zwingend. Falls die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle in einer physischen Schnittstelle zusammenfallen, muss der ST-Autor nachweisen, dass der Konnektor trotzdem die Netze (LAN und WAN) sicher voneinander trennt.

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 muss sicher mit dem EVG verbunden sein. Siehe auch OE.NK.gSMC-K und Abschnitt 7.6.13.

[4] In der Konnektorspezifikation [15] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS2 vorsehen. In diesen Fällen bleibt die Schnittstelle PS3 ungenutzt.

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 (siehe auch Abschnitt 7.6.7).

Anwendungshinweis 11: Der ST-Autor soll die Schnittstellen nach Möglichkeit in Form einer Skizze grafisch darstellen. Dazu kann auch auf die bereits in Abschnitt 1.3.2 enthaltene Abbildung verwiesen werden.

1.3.3.2. Logische Schnittstellen des EVG

Anwendungshinweis 12: Der ST-Autor soll die Beschreibung der logischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Netzkonnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern.

Der EVG besitzt folgende logische Schnittstellen:

LS1 Eine Schnittstelle zum Anwendungskonnektor (Im Fall Mehrboxlösung via PS1).

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

LS3 Eine Schnittstelle zur entfernten Telematikinfrastruktur, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS3[5]) erreicht wird.

LS4 Eine Schnittstelle zum SIS, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS3[6]) erreicht wird.

LS5 Eine Schnittstelle zum ungesicherten Transportnetz, die für den Aufbau der VPN-Kanäle genutzt wird (WAN, via PS3[7]).

LS6 Eine Schnittstelle zu möglicherweise proprietären (herstellerspezifischen) Managementfunktionen des Netzkonnektors (via PS2 oder PS3).

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

Anwendungshinweis 13: Die aktuelle Version der Konnektor-Spezifikation [15], Abschnitt 4.3.8, fordert eine Schnittstelle für entferntes (remote) Management. Dieses muss vom ST-Autor berücksichtigt werden.

[5] In der Konnektorspezifikation [15] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS2 vorsehen.

[6] In der Konnektorspezifikation [15] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS2 vorsehen.

[7] In der Konnektorspezifikation [15] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS2 vorsehen.

1.3.4. Aufbau und physische Abgrenzung des Netzkonnektors

Zur Gesamtarchitektur und für einen Überblick über die Kernkonzepte sei auf die Konnektor-Spezifikation [15] in ihrer jeweils aktuellen Version verwiesen. Eine grobe Abgrenzung des Netzkonnektors von den übrigen Teilen des Konnektors erfolgte bereits in Abschnitt 1.3.

Anwendungshinweis 14: Der ST-Autor soll in diesem Abschnitt die Architektur seines Produkts beschreiben. Dabei soll er sich an der aktuellen Version der Konnektor-Spezifikation [15] orientieren. Siehe auch die Hinweise in Abschnitt 7.6.4 und 7.6.5.

1.3.5. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste

Die im Folgenden beschriebene Sicherheitsfunktionalität stellt die Mindestanforderung an den Netzkonnektor dar: Ein Netzkonnektor (EVG), der dieses Schutzprofil erfüllt, muss mindestens diese Anforderungen erfüllen.

Der EVG erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [15] definierten Schnittstellen weitgehend automatisch. Der EVG ermöglicht ein Management (Administration) nach Autorisierung des Administrators. Die Authentisierung des Administrators kann durch die Umgebung erfolgen.

Anwendungshinweis 15: **Authentisierung des Administrators:** Im Fall einer Einbox-Lösung, die in diesem Schutzprofil angenommen wird, erscheint ein gemeinsamer Administrator-Account für mehrere Konnektorteile wünschenswert. Daher erlaubt dieses Schutzprofil, dass die Authentisierung des Konnektor-Administrators vom NK oder vom AK vorgenommen werden kann. Der jeweils andere Konnektorteil (AK oder NK) kann den Authentisierungszustand übernehmen und auf diese Weise die Zugriffe des Administrators autorisieren. Aufgrund der Annahme A.NK.phys_Schutz ist dabei keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) erforderlich. Das Schutzprofil verbietet nicht, dass der EVG die Authentisierung des Administrators auch selbst durchführen kann; in diesem Fall ist das Umgebungsziel OE.NK.Admin_Auth in ein EVG-Ziel umzuwandeln.

Anwendungshinweis 16: **Vollständigkeit der Dienste:** Die Liste der im Folgenden genannten Dienste ist in dem Sinne vollständig, dass man sich weitere Dienste zwar vorstellen könnte, solche Dienste aber in diesem Schutzprofil bewusst nicht modelliert wurden.

- Beispielsweise erzwingt der VPN-Konzentrator die Nutzung des VPN-Tunnels (er leitet nur Pakete aus dem VPN-Tunnel zu den Fachdiensten weiter). Der Netzkonnektor **unterstützt den VPN-Konzentrator** dabei, indem er das andere Ende des VPN-Tunnels implementiert. Dies stellt aber keine gesonderte Sicherheitsfunktionalität dar, sondern wird bereits unten unter Sicherheitsdienst VPN-Client beschrieben.
- Eine **Vorabprüfung der Datensätze auf Plausibilität** (z. B. XML-Validierung) wird durch den Anwendungskonnektor vorgenommen; dies stellt für den Netzkonnektor keine Sicherheitsfunktionalität dar.
- Eine hohe **Verfügbarkeit des Konnektors** ist natürlich ein wichtiges Ziel im Gesundheitswesen. Bei Nutzung von Infrastrukturen wie z. B. dem Internet kann eine bestimmte Verfügbarkeit jedoch nicht garantiert werden, weil diese von vielen nicht beeinflussbaren Einzelheiten abhängig ist. Daher wurde in diesem Schutzprofil darauf verzichtet, die Verfügbarkeit als Sicherheitsziel (siehe Abschnitt 4.1) zu formalisieren. Gleiches gilt sinngemäß für Quality of Service. Siehe auch Abschnitt 7.6.8. Anforderungen an die Verfügbarkeit von Konnektoren werden im Rahmen des Zulassungsverfahrens für die Konnektoren berücksichtigt.

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

Der EVG erbringt 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 muss die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen erzwingen und ungeschützten Zugriff auf das Transportnetz verbieten. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[8], 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)

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

mit Ausnahme der für den VPN-Verbindungsaufbau erforderlichen Kommunikation[9] sowie Verbindungen zum CRL Download Server.

Anwendungshinweis 18: Bei der Betrachtung von Angriffen aus dem LAN sind auch solche Bedrohungsszenarien zu berücksichtigen, bei denen auf anderen Wegen (z. B. Wechseldatenträger wie CD, DVD, USB-Stick, Diskette) Schadsoftware in die IT-Systeme im LAN des Leistungserbringers kommen kann. Ein **LAN-seitiger Paketfilter** hindert solche Schadsoftware daran, die Integrität des Konnektors zu bedrohen.

Anwendungshinweis 19: Der Netzkonnektor muss kein **Application Layer Gateway** enthalten. 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. Der Verfasser eines konformen STs kann aber auch solche Aspekte ganz oder teilweise in das ST übernehmen.

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 ST-Autor kann optional Maßnahmen zur **Sicherung des Kommunikationskanals** zwischen dem Netzkonnektor und dem zentralen Zeitdienst fordern, sofern dies von der zentralen Infrastruktur unterstützt wird. Als Maßnahmen kommen insbesondere in Frage: (a) Integritätsschutz der übertragenen Zeit und (b) vorherige Authentisierung des zentralen Zeitdienstes gegenüber dem Netzkonnektor. Mindestens gefordert ist eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK. Zu beachten ist, dass die Konnektor-Spezifikation [15] vorsieht, dass die Zeitsynchronisation ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform erfolgt, d.h. über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet. Die Funktionalität soll sich dabei an den aktuellen Versionen der Konnektor-Spezifikation [15] orientieren.

DHCP-Dienst: Der EVG stellt an der LAN-Schnittstelle (PS2) die Funktion eines DHCP Servers gemäß RFC 2131 [35] und RFC 2132 [36] zur Verfügung.

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

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

Gültigkeitsprüfung von Zertifikaten: Der EVG muss die Gültigkeit der Zertifikate des Kommunikationspartners überprüfen, die für den Aufbau eines VPN-Kanals oder TLS-Kanals verwendet werden.[10] 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: Die Prüfung der Algorithmen kann implizit durch den EVG erfolgen, indem sichergestellt wird (z. B. im Rahmen der Evaluierung), dass der EVG nur gültige Algorithmen verwendet. Es ist im Sinne des Schutzprofils zulässig, wenn die Verwendung ungültig gewordener Algorithmen dadurch verhindert wird, dass der EVG entsprechend konfiguriert wird oder dass – unter Verwendung des Software-Update-Mechanismus' des EVGs bzw. des Gesamtkonnektors – ein Update eingespielt wird.

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

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

Darüber hinaus implementiert der EVG folgende übergeordnete Dienste:

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

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

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

Protokollierung: Der EVG führt ein Sicherheits-Log (security log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher muss hinreichend groß dimensioniert sein. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [15].

Anwendungshinweis 24: Die Auswertung des Sicherheits-Logs kann sowohl durch den EVG als auch durch die Einsatzumgebung erfolgen. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

[10] 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.

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 bietet eine lokale Managementschnittstelle an. Teile der Darstellung der Benutzerschnittstelle können dabei durch andere Konnektorteile erbracht werden.

Anwendungshinweis 26: Es soll möglich sein, Wartungsaktivitäten (einschließlich Monitoring und Konfiguration) durchzuführen, ohne den zertifizierten Status des Netzkonnektors zu verlieren (dabei wird davon ausgegangen, dass bei der Wartung die Benutzer- und Administratordokumentation des EVG beachtet wird). Abhängig von der Mächtigkeit der Wartungsschnittstelle sind spezifische Separationsmechanismen erforderlich, welche sicherstellen, dass die Sicherheitsfunktionalitäten des EVG durch die Wartung nicht beeinträchtigt werden. Der ST-Autor kann auch eine Verfeinerung der Komponenten AGD_OPE.1 in Betracht ziehen.

Die Schnittstellen zum lokalen Management des Konnektors sind herstellerspezifisch. Der Umfang der möglichen Wartungsaktivitäten kann unterschiedlich sein. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

Eine Möglichkeit zur Fernwartung ist wünschenswert, wird aber in diesem Schutzprofil nicht verpflichtend gefordert (wohl aber in der Konnektor-Spezifikation [15], Abschnitt 4.3). Falls eine Möglichkeit zur Fernwartung vorhanden ist, muss diese hinreichend gut abgesichert werden. Zur Absicherung der Fernwartung können dieselben oder ähnliche Mechanismen verwendet werden wie zur Absicherung der lokalen Administration an der LAN-Schnittstelle (z. B. sicherer TLS-Kanal zwischen Administrator-Arbeitsplatz und Netzkonnektor wie bei FTP_TRP.1/NK.Admin, Autorisierung des Administrators wie bei FMT_MSA.4/NK). Es ist jedoch zu beachten, dass laut Konnektorspezifikation (Kapitel 4.3.8) bei einer Managementverbindung über die WAN Schnittstelle der Verbindungsaufbau immer vom Konnektor ausgehen muss.

Der EVG erzwingt eine sichere **Authentisierung des Administrators** vor administrativen Aktivitäten. Die Authentisierung selbst kann dabei durch einen anderen Teil des Konnektors (z. B. AK) übernommen werden, der ebenfalls evaluiert wurde. 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 umfasst die Software des Netzkonnektors. Dabei wird der Netzkonnektor immer mit den Konnektorteilen Anwendungskonnektor und der Security Module Card Konnektor gSMC-K gemeinsam betrieben, siehe auch die Beschreibung zur Einsatzumgebung in Kapitel 1.3.2.

Der Netzkonnektor bietet dabei dem Anwendungskonnektor eine sichere Plattform und stellt die in diesem Protection Profile definierten Sicherheitsfunktionen zur Verfügung. Dazu nutzt der EVG die Sicherheitsfunktion der gSMC-K. Das Betriebssystem der gSMC-K muss nach dem Schutzprofil *Card Operating System (PP COS)* [10] evaluiert und zertifiziert sein. Das Objektsystem der gSMC-K muss nach der Technischen Richtlinie TR-03144 [14] evaluiert und zertifiziert sein.

Anwendungshinweis 27: Der Netzkonnektor kann sowohl als reine Software-Lösung implementiert werden als auch in Form einer aus Hardware und Software bestehenden Box, siehe auch Kapitel 7.6.4. Wenn die Hardware nicht Teil des EVGs ist, soll der Verfasser des STs in diesem Kapitel exakte Angaben zur zugrundeliegenden Hardware machen, insbesondere wenn die Hardware zum sicheren Betrieb des EVGs beiträgt (z.B beim sicheren Start des Netzkonnektors). Im Rahmen von ADV_ARC müssen entsprechende Nachweise erbracht werden, dass die Sicherheit des EVGs (unter Berücksichtigung der Einsatzumgebung) durch die Hardware nicht beeinträchtigt wird. Es soll dabei gezeigt werden, dass die Annahme einer sicheren Hardware gerechtfertigt ist. Insbesondere sind kritische Hardware-Komponenten wie zum Beispiel Netzwerkcontroller oder für den sicheren Start relevante Komponenten zu betrachten.

2. Postulat der Übereinstimmung

2.1. Common Criteria Konformität

Das Schutzprofil 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 Schutzprofil:

CC Teil 2 [2] erweitert (extended) und

CC Teil 3 [3] konform (conformant).

2.2. Schutzprofil-Konformität

Dieses Schutzprofil behauptet keine Konformität zu einem anderen Schutzprofil.

2.3. Paket-Konformität

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponente AVA_VAN.5 (Resistenz gegen Angriffspotential „hoch“), ADV_FSP.4 (Vollständige Funktionale Spezifikation), ADV_TDS.3 (Einfaches Modulares Design), ADV_IMP.1 (TSF-Implementierung), ALC_TAT.1 (Wohldefinierte Entwicklungswerkzeuge) und ALC_FLR.2 (Verfahren für Problemreports).

2.4. Begründung der Konformität

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

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

Da das Schutzprofil 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 Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, wie sie in CC Teil 3 [3] definiert ist, zusammen mit der Komponente AVA_VAN.5, um Schutz gegen hohes Angriffspotenzial zu erreichen. Durch direkte und indirekte Abhängigkeiten der Komponente AVA_VAN.5 müssen die Komponenten ADV_IMP.1 und ALC_TAT.1 neu aufgenommen werden und die Komponenten ADV_TDS.3 und ADV_FSP.4 augmentiert werden. Darüber hinaus wurde die Stufe EAL3 noch um die Komponente ALC_FLR.2 augmentiert, die keine

Abhängigkeiten besitzt; für die Gründe dazu siehe Abschnitt 6.6. Die Erweiterung und das Augmentieren von Komponenten ist zulässig.

2.5. Festlegung der Konformität

Sicherheitsvorgaben (Security Targets) und Schutzprofile (Protection Profiles), die Konformität zu diesem Schutzprofil („Schutzprofil 1: Anforderungen an den Netzkonnektor“) behaupten wollen, müssen

strict conformance

behaupten.

2.6. PP-Organisation

Der Aufbau dieses Schutzprofils folgt der Mustergliederung, die durch Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001 [1], Anhang B, vorgegeben wird.

2.7. Hinweise zur Anwendung des PPs

2.7.1. Anwendung des PPs auf unterschiedliche Ausprägungen des EVGs

Dieses Schutzprofil soll als Basis für Evaluierungen unterschiedlicher Ausprägungen des Netzkonnektors dienen können. Das PP soll gleichsam für reine Software-Lösungen und für Lösungen bestehend aus Hardware und Software Anwendung finden. Es soll optional möglich sein, dass ein EVG physischen Schutz bietet, dies wird aber nicht gefordert.

Um diese Allgemeingültigkeit des Schutzprofils zu erreichen, war es erforderlich, die verbindlichen Inhalte im Schutzprofil jeweils auf die Minimalanforderungen an den Netzkonnektor zu beschränken. Jede spezielle Ausprägung des Netzkonnektors kann zusätzliche Sicherheitsanforderungen nach sich ziehen. Wo dies bereits absehbar ist, wird der Leser in diesem Schutzprofil in Form von Application Notes auf diesen Umstand hingewiesen.

Gleichzeitig wurden die Annahmen möglichst vollständig formuliert, damit im ST im Vergleich zum Schutzprofil keine zusätzlichen Annahmen aufgenommen werden müssen. Es steht dem ST-Autor jederzeit frei, in Form von Sicherheitszielen der Einsatzumgebung formulierte Sicherheitsleistungen in EVG-Sicherheitsziele und –anforderungen umzuwandeln.

3. Definition des Sicherheitsproblems

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

Um den Ursprung der hier definierten Bedrohungen, organisatorischen Sicherheitspolitiken sowie der Annahmen zu verdeutlichen, wurden die symbolischen Bezeichner mit dem zusätzlichen Kürzel „NK“ versehen (z.B. eine Annahme „Sichere Telematikinfrastruktur“ wird mit A.NK.sichere_TI bezeichnet). Damit wird die Herkunft dieser Artefakte eindeutig mit „Netzkonnektor“ gekennzeichnet.

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[11] und elektronische Verordnungen (eVerordnungen) sowie sonstige Daten, die im Rahmen der Abwicklung dieser Pflichtanwendungen entstehen (etwa Dispensierdaten).

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

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

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

3.1.1. Primäre Werte

Die primären Werte sind in der folgenden Tabelle 1 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler 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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
Clientsystem, Anwendungs-konnektor	Integrität	Manipulierte Clientsysteme oder Anwendungs-konnektoren können dazu führen, dass zu schützende Daten der TI und der Bestandsnetze abfließen oder unautorisiert verändert werden. Im normalen Betrieb wird davon ausgegangen, dass zu schützende Daten der TI und der Bestandsnetze das Clientsystem nur dann verlassen, wenn sie in die zentrale Telematikinfrastruktur-Plattform oder auf eine eGK übertragen werden sollen. Daher werden zu schützende Daten der TI und der Bestandsnetze nur durch den Anwendungskonnektor bzw. (im Fall von Daten der Bestandsnetze) den Netzkonnektor übermittelt. Ein manipuliertes Clientsystem könnte Kopien der Daten einem Angreifer 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. Siehe auch Abschnitt 7.6.8. ⇒ A.NK.kein_DoS, A.NK.Ersatzverfahren Siehe auch Abschnitt 7.6.8 und Anwendungshinweis 15.

Tabelle 1: Primäre Werte

3.1.2. Sekundäre Werte

Die sekundären Werte sind in der folgenden Tabelle 2 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
Management-Daten (während ihrer Speicherung im	Integrität	Management-Daten (z. B. Konfigurationsdaten) des EVG dürfen nicht unbemerkt verändert werden können, da sonst nicht mehr sichergestellt ist, dass

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
EVG)		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)
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.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
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 2: Sekundäre Werte

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[12] 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 Angreifer kann sich sowohl gegenüber dem Netzkonnektor als (gefälschter) VPN-Konzentrator als auch gegenüber einem VPN-Konzentrator als (gefälschter) Netzkonnektor ausgeben.

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

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

[12] 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.*

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.

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

Der Netzkonnektor muss solche Bedrohungen abwehren, die durch die Einführung der Telematikinfrastruktur neu entstanden sind.

Der Netzkonnektor kann nicht verhindern, dass z. B. ein Einbrecher nachts in eine Arztpraxis eindringt und dort lokal gespeicherte medizinische Daten (z. B. Patientenakten auf Papier oder auch elektronische Patientenakten in ungeschützten Clientsystemen) entwendet – dies war auch vor Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur

schon möglich. Der Netzkonnektor muss aber verhindern, dass Angreifer Zugriff auf Daten neuer Qualität oder neuer Quantität erhalten, etwa durch unbemerktes Mitlesen elektronischer Daten oder durch den unbefugten Zugriff auf Daten in der Telematikinfrastruktur. Die potentiellen Fortschritte für den Angreifer, die es zu verhindern gilt, liegen entweder

- im Datenformat (elektronische Speicherung statt Papier, da so die Kopie, Weiterverarbeitung und Auswertung stark vereinfacht wird)[13],
- in der Datenmenge (Zugriff auf Daten aller Versicherten statt Zugriff auf Daten der Versicherten nur eines Leistungserbringers (z. B. nur einer Arztpraxis), bzw. Zugriff auf alle Daten eines Versicherten (über mehrere Leistungserbringer hinweg) statt Zugriff nur auf die Daten, die bei einem Leistungserbringer über ihn vorliegen),
- in der Tatsache, dass der Zugriff nicht oder nur schwer bemerkt werden kann, so dass evtl. über lange Zeiträume hinweg unbemerkt Daten gesammelt werden können, oder
- in der Tatsache, dass der Angreifer nur einer sehr geringen Gefahr ausgesetzt ist, weil der Angriff z. B. aus dem Ausland über das Internet durchgeführt werden kann, wobei ein deutlich geringeres Risiko der Strafverfolgung besteht.

Die Einführung der Telematikinfrastruktur ist durch folgende Eigenschaften gekennzeichnet:

- Daten liegen in elektronischer Form vor und werden elektronisch gespeichert.
- In der zentralen Telematikinfrastruktur-Plattform werden medizinische und Sozialdaten durchgeleitet.
- Die Übertragung von Daten zwischen Leistungserbringer und zentraler Telematikinfrastruktur-Plattform erfolgt unter Nutzung potentiell unsicherer Transportnetze.

Für den Zugriff aus den lokalen Netzen der Leistungserbringer zu Diensten im Internet kann der NK als Gateway agieren[14]. Durch die Nutzung des Internet sind die Daten und Anwendungen in den lokalen Netzen Gefahren ausgesetzt, die aus den Bedrohungen im Zusammenhang mit Schwachstellen der Systeme, Anwendungen etc. und deren Benutzung resultieren. Der Schutz dieser Komponenten erfolgt nicht durch den NK, sondern durch eine Kombination von Maßnahmen in den lokalen Netzen und Systemen der Leistungserbringer (Virenscanner) mit Maßnahmen am Internet-Zugangspunkt (SIS bzw. Firewall). Im Fall der Nutzung des NK als Gateway muss dieser sicherstellen, dass die übertragenen Daten vom bzw. zum Internet ausschließlich über die Komponente SIS geroutet werden und dass die Vertraulichkeit und Integrität dieser Daten bei der Übertragung zwischen NK und SIS geschützt ist.

Dies führt zu folgenden Angriffspunkten:

[13] Allerdings verarbeiten auch schon vor der Einführung der elektronischen Gesundheitskarte viele HBA-Inhaber Patientendaten elektronisch.

[14] Laut Konnektor-Spezifikation (Kapitel 2.7) [15] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

1. Die Vertraulichkeit oder Integrität von TI-Daten, die in der zentralen Telematikinfrastruktur-Plattform bzw. den Bestandsnetzen gespeichert sind, wird bedroht. Dies kann physisch vor Ort oder logisch über Netzwerkverbindungen erfolgen. Dieser Angriff kann durch den Netzkonnektor nicht verhindert werden, sondern muss durch eine Kombination von lokalen Maßnahmen und Maßnahmen bei der Übertragung durch die VPN Konzentratoren abgewehrt werden.

2. Die Vertraulichkeit oder Integrität von CS-Daten, die lokal beim Leistungserbringer gespeichert sind, wird bedroht. Hier ist insbesondere der Aspekt zu erwähnen, dass die IT-Systeme des Leistungserbringers möglicherweise an unsichere Transportnetze (z. B. Internet) angeschlossen werden können und über diesen Weg Angriffe möglich sind. Der Netzkonnektor muss eine sichere Anbindung an die zentrale Telematikinfrastruktur-Plattform bereitstellen. Zudem muss der Konnektor die Verbindung zwischen dem lokalen Netzen des Leistungserbringers und dem Internet über einen Sicheren Internet Service (SIS) leiten[15].

3. Die Vertraulichkeit oder Integrität von VPN-Daten-TI, die zwischen dem lokalen Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform übertragen werden, wird bedroht. Daten können passiv mitgehört oder sogar aktiv verändert werden. Als Teil eines solchen Angriffs kann beim Etablieren des sicheren Kanals (VPN-Tunnel) zwischen lokalem Leistungserbringer und zentraler Telematikinfrastruktur-Plattform eine falsche Identität vorgetäuscht und auf diese Weise die Vertraulichkeit oder Integrität von Daten kompromittiert werden.

4. Die Vertraulichkeit oder Integrität von VPN-Daten-SIS, die zwischen dem lokalen Leistungserbringer und dem Sicheren Internet Service übertragen werden, wird bedroht. Daten können passiv mitgehört oder sogar aktiv verändert werden. Als Teil eines solchen Angriffs kann beim Etablieren des sicheren Kanals (VPN-Tunnel) zwischen lokalem Leistungserbringer und dem Sicheren Internet Service eine falsche Identität vorgetäuscht und auf diese Weise die Vertraulichkeit oder Integrität von Daten kompromittiert werden.

Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen sind also

- 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-

[15] Dies ist jedoch abhängig vom Einsatz-Szenario und der daraus resultierenden Konfiguration des Konnektors

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 optional auch 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 3 zeigt die beschriebenen externen Einheiten, Objekte und Angriffspfade (nummerierte Pfeile) im Zusammenhang.

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt, da es mehrere topologische Möglichkeiten der Anordnung des Anwendungskonnektors in Relation zum Netzkonnektor gibt (siehe auch Abbildung 2 in Abschnitt 1.3.2 und Abbildung 4 in Abschnitt 7.6.3). Das Kästchen „LAN-Interface“ stellt entweder die Verbindung zum Anwendungskonnektor dar oder schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

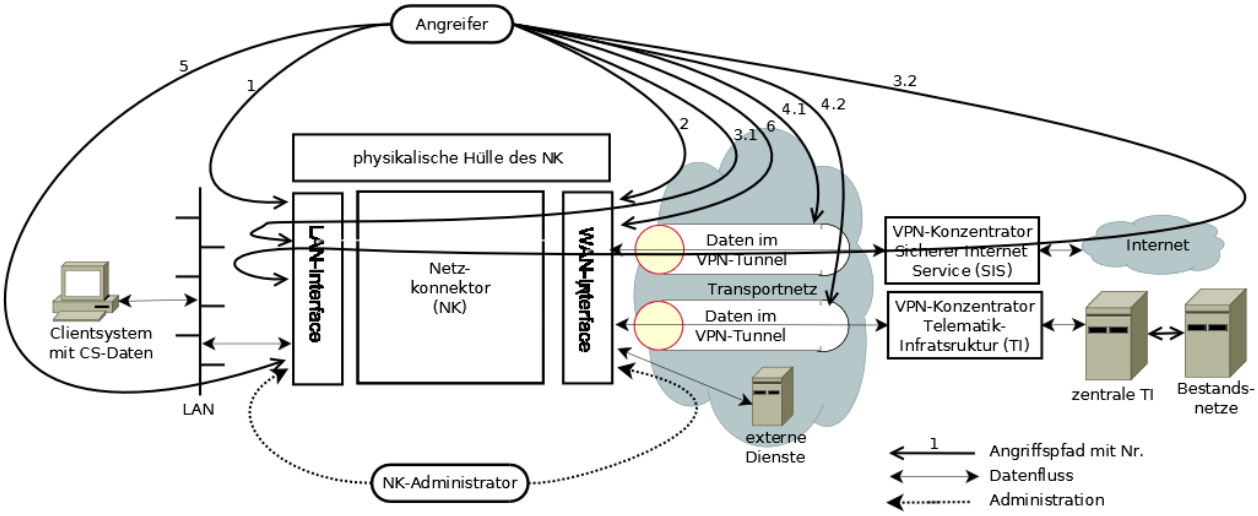

Abbildung 3: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 3 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 3: Kurzbezeichner der Bedrohungen

In den folgenden Abschnitten werden die Bedrohungen genauer beschrieben.

Die Angriffe, deren Bezeichner das Wort „local“ enthalten (T.NK.local_EVG_LAN und T.NK.local_admin_LAN) nehmen an, dass der Angreifer lokal in den Räumlichkeiten des Leistungserbringers agiert, setzen also einen unbefugten physischen Zugriff auf den Netzkonnektor (z. B. Einbruch) voraus. Dabei wird angenommen, dass Personen, die berechtigten Zugang zu vor physischen Zugriff geschützten Bereichen des Leistungserbringers haben, entweder vertrauenswürdig[16] 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

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

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

3.3.2.1. T.NK.local_EVG_LAN

Ein Angreifer dringt lokal in die Räumlichkeiten des Leistungserbringers ein und greift den Netzkonnektor über dessen LAN-Schnittstelle an. Der Angreifer verfügt über hohes Angriffspotential.[17] Ziel bzw. Motivation des Angriffs ist es, den Netzkonnektor zu kompromittieren, um

- im Netzkonnektor gespeicherteskryptographisches 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 Nutzerdatenwährend der Übertragung kompromittiert werden können, oder
- den Netzkonnektor so zu manipulieren, dass zukünftig zu schützende Daten der TI und der Bestandsnetze und zu schützende Nutzerdatenwährend der Übertragung unbemerkt manipuliert werden können.

Für diesen Angriff kann der Angreifer sowohl vorhandene IT-Systeme im LAN des Leistungserbringers nutzen als auch eigene (z. B. Notebook, Netbook, PDA[18], 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: Siehe auch Abschnitt 7.6.17.

---

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

[18] Personal Digital Assistant

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 3 zwei Angriffspfade unterschieden:

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

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

Einen Spezialfall dieses Angriffs (Angriffspfad 3.1 oder 3.2) stellt das Szenario dar, dass ein IT-System im LAN vom Transportnetz bzw. Internet (WAN) aus mit bösartigem Code verseucht wird und in der Folge Angriffe gegen den Konnektor an dessen LAN-seitiger Schnittstelle vornimmt. Ein IT-System im LAN könnte vom Transportnetz aus mit bösartigem Code verseucht werden, wenn der Netzkonnektor keine effektive Netztrennung[19] 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

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

- 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: Siehe auch Abschnitt 7.6.17.

3.3.2.4. T.NK.remote_VPN_Data

Ein Angreifer aus dem Transportnetz hört Daten ab oder manipuliert Daten unbemerkt, die zwischen dem Konnektor und der zentralen Telematikinfrastruktur-Plattform (Angriffspfad 4.2 aus Abbildung 3) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 3) 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[20]. 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.

[20] 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.

3.3.2.8. 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.

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 [13] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [17]. Zudem prüft der EVG die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

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 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.

Im Fall eines verteilt betriebenen Mehrkomponenten-Konnektors schützt die Umgebung außerdem den Kommunikationskanal zwischen den Konnektorteilen Anwendungskonnektor und Netzkonnektor, sowie dem EVG und weiteren Komponenten des Konnektors während aktiver Datenverarbeitung vor physischem Zugriff und erkennt außerhalb aktiver Datenverarbeitung physische Manipulation.

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 nach dem Schutzprofil *Card Operating System (PP COS)* [10] evaluiert und zertifiziert oder bietet gleichwertige Sicherheit, die zum Beispiel

durch eine andere Zertifizierung außerhalb der Gesamtzertifizierung nachgewiesen werden kann. Die Gleichwertigkeit wird im Rahmen der Gesamtzertifizierung überprüft.

Anwendungshinweis 30: Siehe auch Abschnitt 7.6.13.

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: Siehe auch Abschnitt 7.6.8.

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 ST-Autor soll die Funktionalität des EVG und der dazu erforderlichen Separationsmechanismen beschreiben. – Siehe auch Abschnitte 7.6.2 und 7.6.9.

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 ST-Autor soll die Funktionalität des EVG und der dazu erforderlichen Separationsmechanismen beschreiben. – Siehe auch Abschnitte 7.6.2 und 7.6.9.

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 die Telematikinfrastruktur ganz oder teilweise ausfällt oder 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

Um den Ursprung der hier definierten Sicherheitsziele zu verdeutlichen, wurden die symbolischen Bezeichner mit dem zusätzlichen Kürzel „NK“ versehen (z.B. ein Sicherheitsziel „Zeitdienst“ wird mit O.NK.Zeitdienst bezeichnet). Damit wird die Herkunft dieser Sicherheitszeile eindeutig mit „Netzkonnektor“ gekennzeichnet.

4.1. Sicherheitsziele für den EVG

Der EVG muss – wie im Folgenden detaillierter dargestellt – 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 schützen.

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 [13] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [17]. 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 PP 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:** In diesem Schutzprofil wird Schutz vor physischen Angriffen durch die Einsatzumgebung angenommen (siehe A.NK.phys_Schutz). Falls der EVG aus Hardware und Software besteht, kann der ST-Autor optional fordern, dass der EVG physische Angriffe abwehrt oder diese erkennbar macht. In diesem Fall kann die Annahme A.NK.phys_Schutz abgeschwächt werden oder entfallen. Falls der EVG auch Schutz vor physischen Angriffen bieten soll (d.h.: falls der EVG ein sicheres Gehäuse postuliert), umfassen die sicherheitstechnischen Veränderungen in O.NK.Schutz auch physische Manipulationen. Der ST-Autor soll in einem solchen Fall das Ziel O.NK.Schutz im Security Target geeignet erweitern. – Vergleiche zu diesem Themenkomplex auch Abschnitt 7.6.7.

O.NK.EVG_Authenticity Authentizität des EVG

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

Anwendungshinweis 37: Siehe auch Abschnitt 7.6.11.

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 (auf Basis einer in der IT-Umgebung durchgeführten Authentisierung) eines Administrators, welcher die lokale und/oder (optional) 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 muss mindestens die Rolle Administrator unterstützen, bei Bedarf ist auch ein abgestuftes rollenbasiertes Administrationskonzept umzusetzen (getrennte Zugangskennungen, unterschiedliche Administrationsrechte). Der EVG darf auch die Authentisierung selbst vornehmen; in diesem Fall ist O.NK.Admin_EVG geeignet zu verschärfen.

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

Anwendungshinweis 40: Der für die Administration notwendige sichere logische Kanal muss auf den durch [17] vorgegebenen Protokollen und Algorithmen beruhen.

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.

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 der Bundesregierung*, Teil 1: Telematikinfrastruktur [13] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [17] noch gültig sind.

Anwendungshinweis 44: Unter Prüfung der Gültigkeit der verwendeten Algorithmen wird verstanden, dass die Einschränkungen zur Gültigkeit von Algorithmen, die bereits in [13] formuliert sind, durch den EVG durchgesetzt werden. Beispielsweise wird in Version 1.0 des Dokuments „Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur“ [13] in Abschnitt 4.5.2 gefordert, dass für die IPsec-Kommunikation zwischen Konnektor und VPN-Konzentrator „nur langfristig geeignete Kryptoalgorithmen gemäß Kapitel 3“ verwendet werden. Der EVG soll alle in [13] formulierten Anforderungen beachten und die Verwendung der betroffenen Algorithmen geeignet beschränken. Dazu kann der EVG Algorithmen auf Basis der Informationen der Echtzeituhr sperren (siehe OE.NK.Echtzeituhr; optional kann die Echtzeituhr auch im EVG vorhanden sein). Alternativ kann der EVG eine Möglichkeit zur Konfiguration der zulässigen Algorithmen anbieten und die Dokumentation des EVG vorsehen, dass die Verwendung gewisser (nicht mehr zulässiger) Algorithmen ab dem betroffenen Zeitpunkt durch Konfiguration unterbunden wird. Ebenfalls möglich ist die organisatorische Verpflichtung der Leistungserbringer, die innerhalb des Konnektors verwendbaren Algorithmen bei Bedarf durch ein Software-Update auf die zulässige Menge zu beschränken.

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[21] 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.

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

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 Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt[22], 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.

[22] Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [15], Kapitel 2.7.

Anwendungshinweis 46: Siehe auch OE.NK.AK sowie die Abschnitte 7.6.8 (denial-of-service) und 7.6.15 (sichere Kanäle).

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

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

Anwendungshinweis 47: Es ist vorgesehen, den Zufallszahlengenerator der gSMC-K als physikalischen Zufallszahlengenerator der Klasse PTG.2 zu nutzen. Wenn die gSMC-K EVG-Bestandteil ist, geht dieses Sicherheitsziel auf den EVG über. Für den Fall, dass der EVG einen eigenen DRNG bereitstellt, wurde in Abstimmung mit dem BSI eine Liste von „Approved Designs“ erstellt, um den Nachweis der Erfüllung der Anforderungen einer bestimmten Funktionsklasse nach AIS20 [5] zu vereinfachen.

Siehe auch Abschnitt 7.6.12.

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: In der Konnektor-Spezifikation [15] wird gefordert:

„Falls LU_Online nicht aktiviert ist (MGM_LU_Online=Disabled), MUSS sichergestellt werden, dass der maximale zulässige Fehler von +/- 20ppm (part per million) gegenüber einer Referenzuhr nicht überschritten wird. Dies entspricht einer maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über 20 Tage“

Eine solche Annahme ist hilfreich bei der Abschätzung, wie oft die Zeitsynchronisation erfolgen muss, um eine gewisse Genauigkeit des Zeitdienstes garantieren zu können (vgl. das Refinement zu FPT_STM.1/NK). 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: Das Betriebssystem der gSMC-K wird nach dem Schutzprofil *Card Operating System (PP COS)* [10] evaluiert und zertifiziert und das dazugehörige Objektsystem getestet. Der Hersteller des EVG darf nur geeignete evaluierte und zertifizierte Sicherheitsmodule gSMC-K in sein Produkt integrieren. Siehe auch Abschnitt 7.6.13.

OE.NK.KeyStorage Sicherer Schlüsselspeicher

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

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

Anwendungshinweis 50: Der Begriff „Sicherer Schlüsselspeicher“ legt noch keine Implementierungsdetails fest. Es ist auch möglich, dass ein Hersteller für unterschiedliche Schlüssel unterschiedliche Schlüsselspeicher verwendet. Der Begriff wird in diesem Schutzprofil lediglich stellvertretend dafür verwendet, dass Schlüsselmaterial vor unbefugter Kenntnisnahme und Verfälschung geschützt sicher gespeichert wird.

Der NK kann den sicheren Schlüsselspeicher (für seine eigenen Schlüssel) auch selbst bereitstellen.

Anwendungshinweis 51: Optional kann der Schlüsselspeicher auch zur Speicherung von

- Prüfschlüsseln (z. B. öffentlicher Schlüssel) zur Verifikation der eigenen Integrität (diese können alternativ auch in der IT-Einsatzumgebung gespeichert werden, z. B. in der gSMC-K),
- Prüfschlüsseln (z. B. öffentlicher Schlüssel) zur Verifikation der Authentizität von Software-Updates sowie von
- Geheimnissen (z. B. privater Schlüssel) zur Entschlüsselung von Software-Updates, falls diese in verschlüsselter Form übertragen werden und von
- Geheimnissen (z. B. Passwörtern), mit denen der Administrator sich gegenüber dem EVG authentisieren kann (FTP_TRP.1/NK.Admin), falls diese Funktionalität im NK angesiedelt ist sowie vom
- DNSSEC Vertrauensanker der TI (, falls DNSSEC vom DNS-Dienst des EVG unterstützt wird)

verwendet werden.

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 die Abschnitte 7.6.14 und 7.3 (VPN-Konzentrator für den Zugang zur Telematikinfrastruktur).

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: Eine eindeutige Identifikation kann z. B. über eine Seriennummer erfolgen. In diesem Fall muss organisatorisch sichergestellt werden, 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 **Authentisierung des Administrators**

Ein hinreichend vertrauenswürdiges Konnektorteil in der IT-Einsatzumgebung führt eine Authentisierung des Administrators durch.

Anwendungshinweis 54: Beispielsweise könnte der AK die Authentisierung für den EVG durchführen. Die Administrator-Authentisierung wurde im PP [11] als übergreifende Sicherheitsfunktionalität modelliert.

Der EVG kann die Authentisierung aber auch selbst durchführen. In diesem Fall kann das Umgebungsziel OE.NK.Admin_Auth in ein EVG-Ziel umgewandelt werden. Die funktionale Anforderung FMT_MSA.4/NK kann dabei entfallen, sofern stattdessen eine die Authentisierung des Administrators modellierende Anforderung (z. B. eine Komponente aus der Familie FIA_UAU) in das ST aufgenommen wird.

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.

Im Fall eines verteilt betriebenen Mehrkomponenten-Konnektors muss die Umgebung außerdem den Kommunikationskanal zwischen den Konnektorteilen Anwendungskonnektor und Netzkonnektor, sowie dem EVG und weiteren Komponenten des Konnektors während aktiver Datenverarbeitung vor physischem Zugriff schützen und außerhalb aktiver Datenverarbeitung physische Manipulation erkennen.

Anwendungshinweis 55: Siehe auch Abschnitt 7.6.7 und A.NK.phys_Schutz.

OE.NK.sichere_TI Sichere Telematikinfrastruktur-Plattform

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

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

werden müssen und nur für die rechtmäßigen Administratoren zugänglich sein dürfen.

Alle Administratoren in der Telematikinfrastruktur müssen fachkundig und vertrauenswürdig sein.

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

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

Anwendungshinweis 56: Siehe auch Abschnitt 7.6.8.

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 die Telematikinfrastruktur ganz oder teilweise ausfällt oder 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.[23]

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

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

[23] 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.

[24] Laut Konnektor-Spezifikation (Kapitel 2.7) [15] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

4.3. Erklärung der Sicherheitsziele (Security Objectives Rationale)

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

Die folgende Tabelle 4 bildet die Bedrohungen (Threats), organisatorischen Sicherheitspolitiken (OSPs) und Annahmen (Assumptions) auf Sicherheitsziele für den EVG und die Umgebung ab.

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.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.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.Admin_Auth	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
T.NK.local_EVG_LAN		X			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	X
T.NK.local_admin_LAN		X		X	X	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	X	(x)							(x)	
T.NK.counterfeit			X														X							X						X	
T.NK.Zert_Prüf					(x)	(x)		X			(x)		(x)	(x)	(x)	(x)	(x)							X						X	
T.NK.TimeSync					(x)	X	X	X		X	(x)		(x)	X	X	X	X							X						X	
T.NK.DNS					(x)	(x)	X	X			(x)		(x)		(x)	(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																														
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	

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.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.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.Admin_Auth	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
A.NK.Zugriff_gSMC-K																	X										X			

Tabelle 4: 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: Abhängig von der Ausgestaltung des EVG kann sich die **Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen** gegenüber diesem Schutzprofil noch leicht verändern. Der ST-Autor soll die tatsächlichen Produkteigenschaften beschreiben und abhängig davon die Inhalte in Tabelle 4 und im folgenden Erklärungstext (Abschnitte 4.3.1 und 4.3.2) entsprechend anpassen.

Ein in Klammern gesetztes kleines Kreuz (x) bedeutet, dass das Ziel optional zur Abwehr der Bedrohung beitragen kann. Es steht dem ST-Autor frei, entsprechende Beziehungen auszuwählen: Ein in Klammern gesetztes kleines Kreuz (x) kann sowohl gelöscht als auch durch ein großes Kreuz X ersetzt werden.

Werden im Rahmen solcher Anpassungen Beziehungen ergänzt (d. h.: in Tabelle 4 werden Kreuzchen ergänzt), so ist dies kurz zu erläutern. Im Allgemeinen sollten aber keine Beziehungen (bzw. Kreuzchen) gestrichen werden (Ausnahme: Das Löschen kleiner Kreuzchen (x) in Klammern ist zulässig); falls ein großes Kreuzchen X gelöscht werden soll, so ist dies ausführlich zu begründen und mit der Zertifizierungsstelle und ggf. mit der Prüfstelle abzustimmen. Insbesondere ist darauf zu achten, dass alle Bedrohungen weiterhin vollständig und effektiv abgewehrt werden und keine leeren Zeilen oder Spalten entstehen, in denen sich nicht wenigstens ein großes Kreuzchen X befindet.

4.3.2. Abwehr der Bedrohungen durch die Sicherheitsziele

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 4 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 3) 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) kann bei der Abwehr von T.NK.remote_VPN_Data unterstützen, indem auch sicherheitsrelevante Ereignisse im Zusammenhang mit dem VPN-Client protokolliert werden (Schreiben von Sicherheits-Log-Daten zur späteren Auswertung oder forensischen Analyse nach einem Angriff). 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 (OE.NK.Admin_Auth) möglich ist. Die Administratoren halten dazu ihre Authentisierungsinformationen geheim (OE.NK.Admin_EVG) und verhindern so, dass sich ein Angreifer dem EVG gegenüber als Administrator ausgeben kann. Dies wehrt bereits wesentliche Teile des beschriebenen Angriffs ab. Weitere Teilaspekte des Angriffs, insbesondere der Zugriff auf Schlüssel, werden durch weitere Ziele verhindert: Der Zugriff auf kryptographische Schlüssel und andere Geheimnisse im Arbeitsspeicher des EVGs wird durch entsprechende Speicheraufbereitung verhindert (aktives Löschen nach Verwendung der Geheimnisse, O.NK.Schutz). Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage. Administrative Tätigkeiten können im Sicherheits-Log mit Zeitstempel

(O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) nachvollzogen werden (O.NK.Protokoll). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können.

Anwendungshinweis 59: Optional kann auch der Paketfilter gemäß O.NK.PF_LAN bzw. O.NK.PF_WAN und entsprechend die *stateful packet inspection* gemäß O.NK.Stateful zur Abwehr von T.NK.local_admin_LAN bzw. T.NK.remote_admin_WAN beitragen. Ebenfalls optional kann eine PKI in der IT-Einsatzumgebung (OE.NK.PKI) genutzt werden, um den sicheren Kanal für die Administration aufzubauen. Falls im Rahmen der Administration kryptographische Verfahren zum Einsatz kommen (z. B. im Rahmen der Benutzerauthentisierung oder bei der Implementierung eines sicheren Kanals), trägt auch OE.NK.Ersatzverfahren zur Abwehr von T.NK.local_admin_LAN bei. Schließlich kann auch OE.NK.phys_Schutz zur Abwehr von T.NK.local_admin_LAN beitragen, falls 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, OE.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. Optional wirkt auch der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful gegen diese Bedrohung, siehe auch Anwendungshinweis 59.

4.3.2.7. T.NK.counterfeit

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

4.3.2.8. T.NK.Zert_Prüf

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

Anwendungshinweis 60: Optional kann es im Rahmen der Gültigkeitsprüfung von Zertifikaten Plausibilitätsprüfungen geben, welche die Echtzeit des EVG verwenden; somit kann auch O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro zur Abwehr von T.NK.Zert_Prüf beitragen. Optional können auch O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr von T.NK.Zert_Prüf beitragen. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der gSMC-K gespeichert sind, daher kann OE.NK.gSMC-K optional bei der Abwehr von T.NK.Zert_Prüf unterstützen. 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 können. Das Security Target ist entsprechend anzupassen, siehe Anwendungshinweis 57.

4.3.2.9. T.NK.TimeSync

T.NK.TimeSync beschreibt den Angriff, dass Nachrichten manipuliert werden, die im Rahmen einer Zeitsynchronisation mit einem netzbasierten Dienst ausgetauscht werden, um auf dem EVG die Einstellung einer falschen Echtzeit zu bewirken. Dieser Angriff wird durch das Ziel O.NK.Zeitdienst abgewehrt, da dieses die Synchronisation der durch die Umgebung bereitgestellte Echtzeituhr (OE.NK.Echtzeituhr) über einen sicheren Kanal fordert. Weil der Zeitdienst innerhalb der zentralen Telematikinfrastruktur-Plattform bereitgestellt wird, dient bereits der VPN-Tunnel zu dem VPN-Konzentrator für den Zugang zur Telematikinfrastruktur als sicherer Kanal (O.NK.VPN_Integrität). Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Beim Aufbau des Kanals werden die Kummunikationspartner authentisiert (O.NK.VPN_Auth) und Zertifikat geprüft (O.NK.Zert_Prüf) gegen die PKI der TI (OE.NK.PKI). Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der beim VPN-Kanal genutzten kryptographischen Algorithmen richten. Die Zeitserver, die über eine verlässliche Systemzeit verfügen und somit die Basis für eine vertrauenswürdige Zeitinformation im Rahmen der Synchronisierung bilden, werden durch die Umgebung bereitgestellt (OE.NK.Zeitsynchro); außerdem liegen sie innerhalb der Telematikinfrastruktur und bilden somit die Gegenseite des sicheren Kanals.

Anwendungshinweis 61: Auch bei T.NK.TimeSync können optional O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr der Bedrohungen beitragen. Das Security Target ist entsprechend anzupassen, siehe Anwendungshinweis 57.

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[25]. 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, 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

[25] 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.

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 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.

4.3.4. 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 nach einem entsprechenden Schutzprofil evaluiert und zertifiziert ist, und dass der EVG Zugriff auf dieses Modul hat. Der Hersteller des EVG verbaut nur solche zertifizierten Module und die gSMC-K ist sicher mit dem EVG verbunden, so dass die Kommunikation zwischen gSMC-K und EVG weder mitgelesen noch manipuliert werden kann. Somit müssen im Rahmen der Zugriffskontrolle überhaupt nur Zugriffe anderer Konnektorteile (AK) auf die gSMC-K betrachtet werden.

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

5. Definition zusätzlicher Komponenten

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

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

Family **FPT_EMS – EVG Emanation**

Family behaviour This family defines requirements to mitigate intelligible emanations.

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

FPT_EMS.1 – EVG Emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit:FPT_EMS.1

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6. Sicherheitsanforderungen

6.1. Hinweise zur Notation

Der Inhalt dieses Abschnitts ist informativ und nicht zur Übernahme in ein Security Target bestimmt. Der ST-Autor muss aber in ähnlicher Form erläutern, wie er durchgeführte Operationen kenntlich gemacht hat; es steht ihm daher frei, den Text in diesem Abschnitt auszugsweise zu übernehmen und zu überarbeiten.

Die Auswahl der funktionalen Sicherheitsanforderungen basiert auf der zum Zeitpunkt der Erstellung des Schutzprofils aktuellen Version 3.1 Revision 5 der Common Criteria; diese Version [2] liegt in englischer Sprache vor. In diesem Schutzprofil wurden die Formulierungen an Common Criteria Version 3.1 Revision 5 in englischer Sprache beibehalten und die Umsetzung der im Folgenden beschriebenen Operationen in deutscher Sprache durchgeführt.

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

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

Die Operation **Auswahl** (selection) wird genutzt, um eine oder mehrere durch die CC vorgegebenen Optionen auszuwählen. In diesem Schutzprofil wird eine ausgeführte Auswahl durch unterstrichenen Text in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben.

Die Operation **Zuweisung** (assignment) wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Schutzprofil werden Zuweisungen durch *kursiven Text* in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben.

Die Operation **Iteration** wird genutzt, um eine Komponente mit unterschiedlichen Operationen zu wiederholen. In diesem Schutzprofil 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 Schutzprofil wurde zudem das Suffix „NK“ verwendet, selbst wenn keine Iteration vorliegt. Das wurde zur Vereinfachung im Umgang mit der vorgesehenen Evaluierung des Gesamt-Konnektors eingeführt, bei der die in diesem Schutzprofil definierten SFRs wiederverwendet werden sollen.

6.2.1. VPN-Client

VPN

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 (vgl. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS).

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

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

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_TI The TSF shall provide a communication channel between itself and another trusted IT product **VPN-Konzentrator der Telematikinfrastruktur**[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_TI The TSF shall permit the TSF[29] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_TI The TSF shall initiate communication via the trusted channel for *communication with the TI*[30].

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 [15], RFC 4301 (IPsec) [25], RFC 4303 (ESP) [28]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [29]) 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.

---

[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*]

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)**[31] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[32] and protection of the channel data from modification **and**[33] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[34] 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*[35].

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 [15], RFC 4301 (IPsec) [25], RFC 4303 (ESP) [28]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [29]) 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 muss RFC 7296 (IKEv2) [29] unterstützen, siehe [17], Kapitel 3.3.1. Dieser Hinweis bezieht sich auf FTP_ITC.1.1/NK.VPN_SIS und FTP_ITC.1.1/NK.VPN_TI.

---

31 refinement

32 refinement

33 refinement (or → and)

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

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

Anwendungshinweis 63: Eine theoretisch mögliche Kommunikation von EVGs untereinander wird in diesem Schutzprofil nicht behandelt. Falls ein Produkt eine solche Funktionalität bietet, darf sie die Sicherheit der Anwendungen gemäß § 291 a SGB V nicht beeinträchtigen.

Informationsflusskontrolle

Regelbasiert müssen alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel nutzen. 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, müssen den VPN-Tunnel zum Sicheren Internet Service benutzen.

Diese Aspekte ergeben sich zwar aus der Betrachtung der VPN-Kanäle (aufgrund der Frage: Wie wird der Eingang in den VPN-Tunnel geschützt?), 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 unten in Abschnitt 6.2.2) zugeordnet; das „PF“ steht dabei für Paketfilter. Daher finden sich die Anforderungen (SFR) zu diesen Aspekten im nächsten Abschnitt 6.2.2.

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

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Dynamischer Paketfilter

Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird hier als Informationsflusskontrolle modelliert (siehe FDP_IFC.1/NK.PF und die sich daraus ergebenden Abhängigkeiten). Alle funktionalen Anforderungen, die mit dem Paketfilter in direktem Zusammenhang stehen, wurden mit dem Suffix „/NK.PF“ (wie Paketfilter) versehen. Zur zustandsgesteuerten Filterung siehe auch Abschnitt 6.2.4 Stateful Packet Inspection.

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)*[36] on the *subjects*

(1) IAG,

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

(2) VPN concentrator of the TI,

(3) VPN concentrator of the SIS,

(4) the TI services ,

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

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

(7) active entity in the LAN,

(8) CRL download server,

(9) hash&URL server,

(10) registration server of the VPN network provider,

(11) remote management server,

the information

(1) incoming information flows

(2) outgoing information flows

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[37].

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. Siehe auch Abschnitt 7.6.17.

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

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

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der WAN-Adapter des Konnektors angeschlossen ist.

[37] [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_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 Bestandsnetze (ANLW_BESTANDSNETZE)
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
DNS_ROOT_ANCHOR_URL	IP-Adresse des DNSSEC Vertrauensankers für das Internet
hash&URL-Server	IP-Adresse des hash&URL-Servers
registration server	IP-Adresse des Registrierungsservers
remote management server	IP-Adresse des Remote-Managementservers
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
	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=ENABLED befindet sich der EVG in dieser Schaltung. Bei Schaltung [Parallel] befindet sich der EVG als eine von weiteren Komponenten im LAN. Wenn ANLW_WAN_ADAPTER_MODUS=DISABLED befindet sich der EVG in dieser Schaltung.
MGM_LOGICAL_SEPARATION	Parameter aktiviert [Enabled] oder deaktiviert [Disabled] die logische Trennung, wodurch trotz Verbindung des EVG mit dem IAG und darüber mit TI Services eine Verbindung von Clientsystemen mit dem Internet, TI Services und

Konfigurationsparameter	Bedeutung und [Werte]
	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*[38] 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*[39] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES. [40]

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

[39] IP = Internet Protocol

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

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

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

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

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

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

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

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

d) by means of protocol 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

---

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

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≠"").[41]

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*[42].

FDP_IFF.1.4/NK.PF The TSF shall explicitly authorise an information flow based on the following rules*: Stateful Packet Inspection,* [assignment: *rules, based on security attributes, that explicitly authorise information flow*][43].

Refinement: Stateful Packet Inspection (zustandsgesteuerte Filterung) bedeutet in diesem Zusammenhang, dass der EVG zur Entscheidungsfindung, ob ein Informationsfluss zulässig ist oder nicht, nicht nur

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

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

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

jedes einzelne Paket betrachtet, sondern auch den Status einer Verbindung mit in diese Entscheidung einbezieht.

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

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

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

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

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

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

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

(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) [*assignment*: *additional rules, based on security attributes, that explicitly deny information flows*][44].

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.

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: Dazu muss der EVG Informationen über eine (kurze) Historie der Verbindung verwalten. Beispielsweise 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. Der ST-Autor muss die zulässigen Protokolle gemäß Konnektorspezifikation [gemSpec_Kon] [15] und Spezifikation Netzwerk [gemSpec_Net] [16] benennen. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.

Der ST-Autor kann mittels FDP_IFF.1.3/NK.PF bis FDP_IFF.1.5/NK.PF weitere Regeln ergänzen, die der EVG umsetzt. Mindestens sollen die Anforderungen an die in O.NK.PF_LAN beschriebene **Informationsflusskontrolle** an dieser Stelle formuliert werden (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 können weitere Regeln ergänzt werden, etwa weitere Plausibilitätskontrollen; dies ist aber nicht zwingend erforderlich: Bei einem assignment ist auch die Auswahl von *none* zulässig.

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

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*[45] to provide restrictive[46] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [assignment: *the authorised identified roles*] 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: In FMT_MSA.3.2/PF soll der ST-Autor spezifizieren, welche administrativen Rollen alternative Default-Werte spezifizieren dürfen. Denkbar ist insbesondere der lokale Administrator (siehe auch FMT_SMR.1./NK). Das Security Target kann aber auch ein feineres Rollenmodell spezifizieren.

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

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

6.2.3. Netzdienste

Zeitsynchronisation

Der EVG führt in regelmäßigen Abständen eine Zeitsynchronisation mit Zeitservern durch. Siehe auch Sicherheitsdienst Zeitdienst.

---

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

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

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 [20] erreicht.

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

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

Anwendungshinweis 70: Zum Zeitdienst siehe Konnektor-Spezifikation [15], Abschnitt 4.2.5 *Zeitdienst*.

Anwendungshinweis 71: Der ST-Autor soll das Refinement verschärfen, falls die aktuelle Version der Konnektor-Spezifikation [15] eine häufigere Zeitsynchronisation fordert als im Refinement zu FPT_STM.1/NK (einmal innerhalb von 24 Stunden) gefordert. Die Anforderung aus dem Refinement zu FPT_STM.1/NK bleibt in jedem Fall Mindestanforderung, auch für den Fall, dass die Konnektor-Spezifikation weniger strenge Anforderungen formulieren sollte.

Anwendungshinweis 72: Gemäß Konnektor-Spezifikation [15], Abschnitt 3.3 *Betriebszustand*, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [15]

- *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].

Es wird nicht vorgeschrieben, in welchem Konnektorteil sich diese Signaleinrichtung, sofern vorhanden, befindet. **Der ST-Autor muss in jedem Fall an dieser Stelle präzise beschreiben, welche Funktionalität der EVG bietet.** Wenn beispielsweise der Konnektor über eine Signaleinrichtung verfügt, muss hier beschrieben werden, ob der NK die Signaleinrichtung geeignet ansteuert, so dass die Signaleinrichtung vom NK erkannte kritische Betriebszustände korrekt signalisieren kann.

Da sich die logische Clientsystem-Schnittstelle im AK (und nicht im NK) befindet, wurde die Anforderung FPT_FLS.1 im Schutzprofil [11] formuliert.

Die Aufgabe des NKs (EVG in diesem Schutzprofil) beschränkt sich darauf, den Umstand einer nicht erfolgten Zeitsynchronisation geeignet dem AK zu melden, so dass dieser via Ereignisdienst seine Benutzer informieren kann, bzw. optional (falls eine zusätzliche Signaleinrichtung vorhanden ist) den Umstand auch dem Konnektorteil zu melden, welches über die Signaleinrichtung verfügt, so dass die Signaleinrichtung den kritischen Betriebszustand anzeigen kann.

Aufgrund dieser Beschränkung wurde der Aspekt der Meldung kritischer Betriebzustände an den Benutzer in diesem Schutzprofil nicht mittels FPT_FLS.1, sondern als Verfeinerung zu FPT_STM.1 modelliert. **Die Anforderung FPT_STM.1 umfasst also die Korrektheit der Kommunikation zwischen dem NK und anderen Konnektorteilen (ggf. Signaleinrichtung); diese Kommunikation ist im Rahmen der Evaluierung des NKs zu prüfen und zu testen.**

Zertifikatsprüfung

Der EVG muss die Gültigkeit der Zertifikate überprüfen, 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.

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

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[48] when interpreting the TSF data from another trusted IT product.

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

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

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

Anwendungshinweis 73: Der ST-Autor soll die *interpretation rules* in FPT_TDC.1.2/NK.Zert geeignet verfeinern; dazu soll er sich an der aktuellen Version der Konnektor-Spezifikation [15] orientieren.

Anwendungshinweis 74: Die TSL und die CRL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [15] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden.

Der Konnektor kann die TSL und die CRL bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [15]).

6.2.4. 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. Siehe auch Anwendungshinweis 23.

Anwendungshinweis 75: Weitergehende Angriffe gegen die Systemintegrität des EVG müssen abgewehrt werden (robuste Implementierung, Resistenz gegen Angriffe wie von AVA_VAN.5 gefordert), aber nicht im Detail erkannt werden (es wird keine komplexe Erkennungslogik für Angriffe gefordert).

Es steht dem ST-Autor frei, im Security Target weitergehende Funktionalität als Differenzierungsmerkmal zu fordern.

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

6.2.5. Selbstschutz

Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren.

Speicheraufbereitung

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

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[49] 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),* [assignment: *list of objects*][50].
Refinement:	Die sensitiven Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. Reset überschrieben werden.

Anwendungshinweis 76: Wann Daten nicht mehr benötigt werden und somit aktiv überschrieben werden müssen, soll sinnvoll festgelegt werden; dabei sollten weitere Aspekte wie Performance und Vermeidung unnötig häufiger Schlüsselableitungen berücksichtigt werden. Der Konnektor speichert *zu schützende Daten der TI und der Bestandsnetze* oder *zu schützende Nutzerdaten* niemals dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z. B. während einer Ver- oder Entschlüsselung). Das offene Assigment des Elements FDP_RIP.1.1/NK darf leer sein

Selbsttests

Der EVG bietet seinen Benutzern eine Möglichkeit, die eigene Integrität zu überprüfen.

FPT_TST.1/NK TSF testing

	Selbsttests
Dependencies:	No dependencies.
FPT_TST.1.1/NK	The TSF shall run a suite of self tests [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*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[51].
FPT_TST.1.3/NK	The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*] .
Refinement:	Zur Erfüllung der Anforderungen aus FPT_TST.1/NK muss der EVG mindestens die Mechanismen implementieren, welche dem aktuellen Stand der Technik bei Einzelplatz-Signaturanwendungen entsprechen. Dazu gehören insbesondere: • die Prüfung kryptographischer Verfahren bei Programmstart,

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

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

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

- eine Prüfung der korrekten Funktionalität und Qualität des RNG, sofern der EVG einen physikalischen Zufallszahlengenerator beinhaltet und diesen anstelle des Umgebungsziels OE.NK.RNG nutzt.

Anwendungshinweis 77: Beispiele für die im Refinement geforderten Mechanismen sind:

- Eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (z. B. Konfigurationsdateien, TSF-Daten) mit kryptographischen Verfahren beim Programmstart sowie
- die Möglichkeit, einen aussagekräftigeren Test mit einem externen Vertrauensanker manuell anzustoßen (z. B. von CD-ROM oder schreibgeschütztem USB-Stick ablaufender Test: Das Medium enthält in diesem Fall das Testprogramm und die gültigen Hashwerte bzw. Signaturen).

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). Dies gilt grundsätzlich für *kryptographisches Schlüsselmaterial* (siehe Tabelle 2: Sekundäre Werte in Abschnitt 3.1.2). Zur Definition der Anforderung FPT_EMS.1/NK siehe Abschnitt 5.1.

Der private Authentisierungsschlüssel für das VPN wird bereits durch die gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG soll darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll verhindern, etwa Session Keys oder sonstige Informationen, die sich aus dem Protokoll im Rahmen des IPsec-Kanalaufbaus ergeben könnten.

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,*
- *[selection: none, key material used to verify the TOE's integrity during self tests],*
- *[selection: none, key material used to verify the integrity and authenticity of software updates],*
- *[selection: none, key material used to decrypt encrypted software updates (if applicable)],*

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

[53] [assignment: *specified limits*]

- *[selection: none, key material used for authentication of administrative users (if applicable)]*,
- *[assignment: list of other types of TSF data (may be empty)]*[54] and
- *data to be protected (“*zu schützende Daten der TI und der Bestandsnetze”)
- *[assignment: list of types of user data (may be empty)]*[55].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)*[56] are unable to use the following interface *WAN interface or LAN interface of the connector*[57] to gain access to **the sensitive data (TSF data and user data) listed above**[58].

Anwendungshinweis 78: Der ST-Autor kann hier weitere Verfeinerungen vornehmen. Siehe auch Abschnitt 7.6.16.

Sicherheits-Log

Der EVG führt ein Sicherheits-Log wie unter Sicherheitsdienst *Protokollierung* in Abschnitt 1.3.5 beschrieben. Vergleiche dazu auch die Konnektor-Spezifikation [15], Abschnitt 4.1.10.

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

---

54 [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. Siehe auch Abschnitt 7.6.16.

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

56 [assignment: *type of users*]

57 [assignment: *type of connection*]

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

- *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.*[59]

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

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

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

Anwendungshinweis 79: Der ST-Autor soll die Liste in FAU_GEN.1.1/NK.SecLog, Punkt c) in Abstimmung mit der Zertifizierungsstelle und der Konnektor-Spezifikation [15] (Abschnitte 3.2 und 3.3, Tabelle 3) abgleichen. 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". Wenn der Protokollierungsdienst als erster Dienst gestartet wird, so kann dieser Zeitpunkt als Zeitpunkt für das Ereignis „start-up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet werden. Wenn der Protokollierungsdienst als letzter Dienst bei einem Shut-down des EVG beendet wird, so kann dieser Zeitpunkt als Zeitpunkt für das Ereignis „*shut down*“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet werden.

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

Anwendungshinweis 80: Die exakte Größe des für das Security Log zu reservierenden Speicherbereichs ist somit abhängig von der Größe der einzelnen Log-Einträge, von der verwendeten Kodierung (z. B.: Ereignismeldung im Klartext als ASCII-kodierter String der Länge 80 Zeichen vs. Kodierung des Ereignistyps als Nummer in einem Byte) und weiteren Produkteigenschaften, beispielsweise vom eventuellen Vorhandensein optionaler Auswertelogik, welche bewusste Verdrängungsversuche während der Protokollierung erkennt und verhindert. Stößt ein Angreifer beispielsweise wiederholt dieselbe Aktion an, die zu einem Log-Eintrag führt, könnte der EVG nach einer gewissen Anzahl dazu übergehen, nur noch die Anzahl der Ereignisse zu zählen und nicht für jedes Ereignis einen vollständigen Log-Eintrag zu schreiben. Dabei muss jedoch sichergestellt sein, dass die geforderten Informationen weiterhin verfügbar sind. Beispiel: Es gab 1846 fehlgeschlagene Login-Versuche als Administrator, davon die ersten zehn zu folgenden Zeiten (Datum und Uhrzeit), die letzten 50 zu folgenden Zeiten (Datum und Uhrzeit) und die übrigen in regelmäßigen Abständen (oder: gehäuft immer gegen Mitternacht).

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 muss bei Konfigurationsänderungen durch authentisierte Administratoren die Identität des ändernden Administrators in das Sicherheits-Log aufnehmen. Falls der EVG mehrere Administrator-Rollen unterstützt, soll der Sicherheits-Log-Eintrag die jeweilige Administrator-Rolle eindeutig identifizieren.

6.2.6. Administration

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

Der EVG verwaltet mindestens eine Administrator-Rolle (FMT_SMR.1./NK). Der Administrator muss autorisiert sein (FIA_UID.1/NK.SMR, FMT_SMR.1./NK und FMT_MSA.4/NK), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1/NK). Die Authentisierung kann dabei durch die Einsatzumgebung (z. B. durch die Signaturanwendung des Konnektors) erfolgen, siehe OE.NK.Admin_Auth.

Die Wartung selbst erfolgt unter der Annahme, dass der Administrator über Netzwerkverbindungen (z. B. LAN) zugreift, stets über einen sicheren Pfad (siehe FTP_TRP.1/NK.Admin).

Die administrativen Tätigkeiten bzw. Wartungstätigkeiten werden in FMT_SMF.1/NK aufgelistet. Die Administration der Filterregeln für den dynamischen Paketfilter (siehe oben: FDP_IFC.1/NK.PF) ist den Administratoren vorbehalten (FMT_MSA.1/NK.PF).

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*[60].

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

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

Anwendungshinweis 82: Der EVG unterstützt die Rolle Administrator.

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

FMT_MTD.1.1/NK The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clear*, [assignment: *other operations*]] the *real time clock*, *packet filtering rules [assignment: list of other TSF data (may be empty)]*[61] to *the role Administrator*[62].

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.

60 [assignment: *the authorised identified roles*]

61 [assignment: *list of TSF data*]

62 [assignment: *the authorised identified roles*]

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

Anwendungshinweis 85: Falls der EVG ein **Deaktivieren der VPN-Verbindung** erlaubt, darf nur der Administrator dieses Deaktivieren vornehmen. Dazu soll der ST-Autor die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ in die Liste bei FMT_SMF.1/NK aufnehmen und innerhalb von FMT_MTD.1/NK den Zugriff auf diese Managementfunktion auf den Administrator beschränken.

FIA_UID.1/NK.SMR Timing of identification

Identification of Security Management Roles

Dependencies: No dependencies.

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

- *all actions except for administrative actions (as specified by FMT_SMF.1*/NK*, see below)*[63]

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: Der ST-Autor darf die Zuweisung *all actions except for administrative actions (as specified by FMT_SMF.1*/NK*)* im Sinne eines Refinement verändern, d.h., er darf im Security Target eine weniger umfangreiche Menge von Aktionen (*TSF-mediated actions*) anstelle der hier vorgenommenen Auswahl zuweisen. Vor administrativen Tätigkeiten muss die Identifikation verpflichtend bleiben.

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 [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*].

FTP_TRP.1.2/NK.Admin The TSF shall permit [selection: *the TSF*, *local users, remote users*] 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*.[64]

---

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

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

Anwendungshinweis 87: Der ST-Autor kann sich durch die Selection remote / local aussuchen, ob die Wartung über die LAN-Schnittstelle (PS2) und/oder über die WAN-Schnittstelle (PS3) erfolgen kann. Abhängig davon, wie der EVG gewartet werden kann, soll der ST-Autor die Selection vornehmen.

FMT_SMF.1/NK Specification of Management Functions

Dependencies: No dependencies.

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

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

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

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.) [65]

Anwendungshinweis 88: Optional kann der EVG auch das Review (Lesen und Auswerten) der von FAU_GEN.1/NK.SecLog erzeugten Audit-Daten als Managementfunktion anbieten.

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*[66] to restrict the ability to *[selection: query, modify, delete, [assignment: other operations]]*[67] the security attributes *packet filtering rules*[68] to *the roles*

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

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

[67] **[**selection: *change_default, query, modify, delete, [assignment: other operations]*] (die Auswahl (selection) wurde in dem Sinne ausgeführt, dass die Auwahlmöglichkeiten beschränkt wurden)

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

„Administrator“, [assignment (may be empty): other authorised identified roles][69].

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

– die Kommunikation zwischen dem Konnektor einerseits und dem Transportnetz, der Telematikinfrastruktur, sowohl gesicherte als auch offene Fachdienste und zentrale Dienste, bzw. den Bestandsnetzen andererseits oder

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

betreffen, dürfen nicht über die Administrator-Schnittstelle verändert werden können. Der Administrator muss den gesamten WAN-seitigen Verkehr blockieren können (siehe Konnektorspezifikation [15], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [15], 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 [15] 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.

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

Anwendungshinweis 89: Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [15] definierten Anforderungen.

Anwendungshinweis 90: Eine Möglichkeit, Firewall-Regeln zu aktualisieren, besteht darin, ein **Software-Update** einzuspielen (grundsätzlich im Rahmen der Auslieferung einer neuen Version des EVGs – oder aber als zusätzliche, optionale Funktionalität des EVGs; siehe unten).

Alternativ und abhängig von der Realisierung kann aber auch eine andere kompetente Instanz als weitere Rolle des Netzkonnektors in FMT_SMR.1./NK modelliert werden. Der ST-Autor muss beschreiben, welche Funktionalität der NK bietet.

Denkbar wäre etwa, dass Filterregeln als signierte Pakete ebenfalls per Software-Download bezogen werden können. An die Prüfung solcher Pakete von Filterregeln und deren Signatur wären entsprechend hohe Umgebungsanforderungen zu stellen, da die Sicherheit des EVG durch Möglichkeiten zur missbräuchlichen Verteilung manipulierter Filterregel-Updates unmittelbar und hochgradig gefährdet wäre.

Sofern Filterregeln vom EVG als eine eigene Art von Update erkannt und unterschieden werden, kann ein Update von Filterregeln als Update von TSF-Daten angesehen werden (eine Art Administration durch einen weiteren, anderen „Administrator“, der sich nicht durch ein Passwort authentisiert, sondern durch korrekte Signaturen unter seinen Filterregel-Updates). Somit wäre bei einem Update der Filterregeln nicht zwangsläufig eine Re-Evaluierung des EVG erforderlich.

Anwendungshinweis 91: Das Schutzprofil verbietet es nicht, dass der Netzkonnektor seine Filterregeln abhängig von Ereignissen anderer Konnektorteile (z. B. Anwendungskonnektor) dynamisch anpasst (Beispiel: Operation *subscribe* beim cetp-Protokoll).

FMT_MSA.4/NK Security attribute value inheritance

Definition von Regeln für die Sicherheitsattribute

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

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

Die Authentisierung des Administrators kann gemäß OE.NK.Admin_Auth in der IT-Einsatzumgebung erfolgen.

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

Wenn die Authentisierung des Administrators in der IT-Einsatzumgebung erfolgt und nicht erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diesen Status und weisen dem Sicherheitsattribut „Autorisierungsstatus“ des auf diese Weise

*nicht authentisierten Benutzers „Administrator“ den Wert „**nicht autorisiert**“ zu.*[70]

Subjekt	Sicherheitsattribut	Mögliche Werte
Administrator	Autorisierungsstatus	autorisiert, nicht autorisiert

6.2.7. Kryptographische Basisdienste

Der Konnektor soll laut Dokument „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt]“ [17] die im Folgenden aufgelisteten kryptographischen Primitive implementieren.

Anwendungshinweis 92: Die SFR der Familie FCS in CC Teil 2 [2] enthalten ein [assignment: *cryptographic algorithm*]. Diese Zuweisungen wurden in den SFR dieses Kapitels in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI 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 [17] 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 Schlüsselmanagementfunktionen implementieren muss. Die Anforderungen an die Gewährleistung der Interoperabilität sind hiervon nicht betroffen.

Anwendungshinweis 93: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Bezüglich der Zulässigkeit der Nutzung einer zusätzlichen im Rahmen der Evaluierung nach diesem PP nicht untersuchten AES-Implementierung gelten die Aussagen der Technischen Richtlinie BSI TR-03116-1 [13]. In jedem Fall muss der TOE stets den Wechsel zur geprüften AES-Implementierung durch den Administrator ermöglichen und diese als Voreinstellung vorsehen. Die korrekte Funktion des Wechsels ist im Rahmen der Evaluierung zu dokumentieren.

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

[70] [assignment: *rules for setting the values of security attributes*] (die Schriftauszeichnungen im Zuweisungstext dienen der besseren Leserlichkeit und kennzeichnen hier keine ausgeführten Operationen)

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*[71] in accordance with a specified cryptographic algorithm *SHA-1, SHA-256, [assignment: list of SHA-2 Algorithms with more than 256 bit size]*[72] and cryptographic key sizes *none*[73] that meet the following: *FIPS PUB 180-4 [23]*.[74]

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*[75] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, [assignment: list of SHA-2 Algorithms with 256bit size or more]*[76] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *FIPS PUB 180-4 [23], RFC 2404 [32], RFC 4868 [33], RFC 7296 [29]*.[77]

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

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

[72] [assignment: *cryptographic algorithm*]

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

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

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

[76] [assignment: *cryptographic algorithm*]

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

FCS_CKM.1 Cryptographic key generation]

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

FCS_CKM.4 Cryptographic key destruction

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 operation* [78]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[79] and cryptographic key sizes *2048 bit*[80] that meet the following: *RFC 8017 (PKCS#1) [22], FIPS PUB 180-4 [23]*[81].

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*[82] in accordance

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

[79] [assignment: *cryptographic algorithm*]

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

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

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

with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42)*[83] and cryptographic key sizes *256 bit*[84] that meet the following: *FIPS 197 [24], RFC 3602 [31], RFC 4303 (ESP) [28],], specification [17]* [85].

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*[86] in accordance with a specified cryptographic algorithm *IPsec-protocol*[87] and cryptographic key sizes *256 bit*[88] that meet the following: *RFC 4301 (IPsec) [25], specification [17]*[89].

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 [assignment: *cryptographic key generation algorithm*] and specified

[83] [assignment: *cryptographic algorithm*]

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

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

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

[87] [assignment: *cryptographic algorithm*]

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

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

cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *specification [17], TR-03116 [13]*[90].

Anwendungshinweis 94: 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 Schutzprofil wurde eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols seine Sitzungsschlüssel (*session keys*) für die VPN-Kanäle ableitet; diese Ableitung wird als Schlüsselgenerierung angesehen. (Der Aspekt des Schlüsselaustausches mit einem VPN-Konzentrator wird als FCS_CKM.2/NK.IKE modelliert, siehe unten). Alle erzeugten Schlüssel müssen mindestens 100 bit Entropie besitzen, damit der EVG resistent gegen Angriffe mit hohem Angriffspotential sein kann.

FCS_CKM.2/NK.IKE Cryptographic key distribution

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.2.1/NK.IKE The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *IPsec IKE v2*[91] that meets the following *standard: RFC 7296 [29], specifications [17], TR-02102-3 [12]*[92].

FCS_CKM.4/NK Cryptographic key destruction

Löschen nicht mehr benötigter Schlüssel.

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

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

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

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

FCS_CKM.4.1/NK The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Anwendungshinweis 95: 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. Der ST-Autor soll spezifizieren, wie die Schlüssel zerstört werden. Das Überschreiben der Schlüssel mit festen oder zufälligen Werten kann ein zulässiges Verfahren darstellen.

Anwendungshinweis 96: Der ST-Autor soll eventuelle Verfeinerungen der Zuweisungen der Operationen im Einklang mit den in Dokumenten [13], [17] und [15] vornehmen. Dieser Hinweis gilt für alle genannten SFRs FCS_COP.1/* sowie FCS_CKM.1/NK, FCS_CKM.2/NK.IKE und FCS_CKM.4/NK. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle definierten Kryptoverfahren.

Der DH-Exponent für den Schlüsselaustausch soll eine Mindestlänge gemäß [17] aufweisen. Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy sind die Vorgaben aus [17] zu beachten.

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

Hinweis 1: Tatsächlich verwendet werden die von der Spezifikation geforderten TLS-Verbindungen erst im Anwendungskonnektor. Daher sollte die Aufnahme der folgenden SFRs nicht so interpretiert werden, dass ein Hersteller deshalb die Architektur seines Produktes anders gestalten soll, als er es ohne diese Änderung getan hätte.

Hinweis 2. Es ist denkbar, dass ein Hersteller weitere TLS-Verbindungen implementiert, die über die in der gematik-Spezifikation geforderten hinausgehen. Ein Beispiel wäre die Absicherung einer Administrationsschnittstelle des Netzkonnektors mittels TLS. In diesem Fall kann der Hesteller die SFRs in diesem Kapitel dafür mit nutzen und sie entsprechnd vervollständigen oder durch weitere SFRs ergänzen. Bei einigen SFRs wurden zu diesem Zweck Operationen offen gelassen, um zusätzliche Anforderungen für solche TLS-Verbindungen integrieren zu können.

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**[93] provide~~s~~ assured identification of its end points and protection of the channel data from modification **and**[94] disclosure.

FTP_ITC.1.2/NK.TLS The TSF **must be able to**[95] permit *the TSF or another trusted IT-Product*[96] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.TLS The TSF shall initiate communication via the trusted channel for *communication required by the Anwendungskonnektor, [assignment: list of other functions for which a trusted channel is required]*[97].

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 [15] und [17], wobei TLS 1.2 gemäß RFC 5246 [38] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,

TLS_DHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

TLS_ECDHE_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 Authentitisierung eines der

---

93 refinement: dieses Refinement soll darauf hinweisen, dass der Netzkonnektor die Möglichkeit implementiert, beide Seiten zu authentisieren, dass es aber Entscheidung des nutzenden Systems (i.a. der Anwendungskonnektor) ist, inwieweit diese Authentisierung genutzt wird.

94 refinement (or → and)

95 refinement (shall → must be able to)

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

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

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 97: Der EVG muss TLS Version 1.2 [38] unterstützen und kann zusätzlich TLS Version 1.3 [37] unterstützen (s. [17]). Der EVG muss alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS unterstützen, dabei müssen die Anforderungen aus [17] erfüllt werden. Die Kryptosuiten sollen für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt werden. Der Konnektor darf TLS Version 1.0 und 1.1 sowie SSL nicht unterstützen.

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) [assignment: additional list of data types][98]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS_Zert The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*][99] 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.

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

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

Anwendungshinweis 98: Der ST-Autor soll gegebenenfalls die *interpretation rules* geeignet verfeinern; dazu soll er sich an der aktuellen Version der Konnektor-Spezifikation [15] orientieren.

Anwendungshinweis 99: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [15] 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 [15]).

FCS_CKM.1/NK.TLS Cryptographic key generation / TLS

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

hier erfüllt durch: FCS_COP.1/NK.TLS.HMAC und FCS_COP.1/NK.TLS.AES

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_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[100]
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*[101] that meet the following: *Standard RFC 5246 [38]*.[102]

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

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

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

Anwendungshinweis 100: Der EVG muss TLS Version 1.2 [38] unterstützen und kann TLS Version 1.3 [37] unterstützen (s. [17]). Wird TLS 1.3 unterstützt muss der Autor des ST die SFR FCS_CKM.1/NK.TLS um den entsprechenden Standrad erweitern. Der EVG muss alle im SFR genannten cipher suites als Algorithmen für TLS unterstützen. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [40]) bzw. dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (ECDHE_RSA nach [41]). Die Auswahloperation zur Schlüssellänge hängt von den gewählten Algorithmen ab. Die Schlüssel sollen für die TLS-Kommunikation zwischen dem EVG und anderen Komponenten genutzt werden. 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 muss Schlüssel mit einer Entropie von mindestens 100 Bit erzeugen (siehe [13]). Bezüglich Diffie-Hellman-Gruppen für die Schlüsselaushandlung sind die Vorgaben aus [17] zu beachten. Der DH-Exponent für den Schlüsselaustausch soll eine Mindestlänge gemäß [17] aufweisen. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange müssen die gemäß [17] vorgegebenen Kurven unterstützt werden.

FCS_COP.1/NK.TLS.HMAC Cryptographic operation / HMAC for TLS

Zu unterstützende Hash basierende MAC-Algorithmen

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.HMAC The TSF shall perform *HMAC value generation and verification*[103] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[104] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[105] that meet the following: *Standards FIPS 180-4 [23] and RFC 2104 [43]*[106].

Anwendungshinweis 101: FCS_COP.1/NK.TLS.HMAC wird für die Integritätssicherung innerhalb des TLS-Kanals benötigt.

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

[104] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/NK.TLS.AES Cryptographic operation

Zu unterstützende Verschlüsselungs-Algorithmen für die TLS Verbindung in FTP_ITC.1/NK.TLS

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.AES The TSF shall perform *symmetric encryption and decryption*[107] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[108] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[109] that meet the following: *FIPS 197 [24], NIST 800-38D [39], RFC 5246 [38], RFC 8422 [41], RFC 5289 [42], specification [17]* [110].

Anwendungshinweis 102: Es gilt Anwendungshinweis 93.

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 von der gSMC-K bzw. SM-B durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K bzw. SM-B. 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

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

[108] [assignment: *cryptographic algorithm*]

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

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

entsprechenden 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 storing the signing key and performing the RSA operation* [111]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[112] and cryptographic key sizes *2048 bit*[113] that meet the following: *RFC 8017 (PKCS#1) [22], FIPS PUB 180-4 [23]*[114].

Anwendungshinweis 103: Die Signaturberechnung gemäß FCS_COP.1/NK.TLS.Auth wird für die Berechnung digitaler Signaturen zur Authentisierung bei TLS verwendet. Der EVG nutzt dafür bei Verbindungen ins lokale Netz (LAN) des Leistungserbringers die gSMC-K. Der dafür benötigt asymmetrische Schlüssel kann während der Produktion der gSMC-K importiert oder generiert werden. Es werden deshalb keine spezischen Anforderungen an die Quelle dieses Schlüssels gestellt. 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

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

[112] [assignment: *cryptographic algorithm*]

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

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

FCS_CKM.1.1/NK.Zert The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment**:** *Algorithm for cryptographic key generation of key pairs*] and specified cryptographic key sizes *2048 bit*[115] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [21], BSI TR-03116-1 [13]*[116].

The TSF shall

(1) create a valid X.509 [44] certificate with the generated RSA key pair and

(2) create a PKCS#12 [45] file with the created certificate and the associated private key. [117]

Anwendungshinweis 104: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [17], Anforderung GS-A_4368 umsetzen. Die Verfeinerung zu FCS_CKM.1/NK.Zert soll die Möglichkeit zur Erzeugung von X.509 Zertifikaten für die TLS-geschützte Kommunikation mit Clientsystemen bieten. Ein Export dieser Zertifikate und der zugehörigen privaten Schlüssel ist Gegenstand von FDP_ETC.2/NK.TLS.

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.

[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*[118] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

[117] refinement

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

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) [assignment: *additional importation control rules]*. [119]

Anwendungshinweis 105: Gemäß FMT_MOF.1/NK.TLS kann der Netzkonnektor die Steuerung, unter welchen Umständen der Import von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen. Wenn es für den Hersteller aber einfacher ist, dies im Kontext des Netzkonnektors zu beschreiben (etwa weil er eine vom Netzkonnektor gemanagede Schnittstelle dafür verwendet) ist auch dies gemäß FMT_MOF.1/NK.TLS zulässig.

FDP_ETC.2/NK.TLS Export of user data with security attributes

Export von Zertifikaten

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

nicht erfüllt mit folgender Begründung: Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanagt. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen erzeugt und exportiert werden. Damit wird diese Abhängigkeit inhaltlich erfüllt.

FDP_ETC.2.1/NK.TLS The TSF shall enforce the *Certificate-Export-SFP*[120] 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.

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

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

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) [assignment: additional exportation control rules]. [121]

Anwendungshinweis 106: Gemäß FMT_MOF.1/NK.TLS kann der Netzkonnektor die Steuerung, unter welchen Umständen der Export von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen. Wenn es für den Hersteller aber einfacher ist, dies im Kontext des Netzkonnektors zu beschreiben (etwa weil er eine vom Netzkonnektor gemanagede Schnittstelle dafür verwendet) ist auch dies gemäß FMT_MOF.1/NK.TLS zulässig.

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[122] the functions *Management of TLS-Connections required by the Anwendungskonnektor*[123] to *Anwendungskonnektor*[124].

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.**

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

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

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

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

4. **Whether a "Keep-Alive" mechanism is used for a connection.**
5. **Which data can or must be transmitted via each TLS-Connection.**
6. **Whether the validity of the certificate of a remote IT-Product needs to be verified and whether a certificate chain or a whitelist is used for this verification.**
7. **Under which conditions a TLS-connection is terminated.**
8. **Whether and how terminating and restarting a TLS-connection using a Session-ID is allowed.**
9. **Whether and under which conditions certificates and keys for TLS-Connections are generated and exported or imported.**
10. **[assignment: *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. [125]

Anwendungshinweis 107: 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.

Das assignment „additional rules" soll dem Verfasser des ST die Möglichkeit geben, weitere Handlunsoptionen für einen Anwendungskonnektor zu beschreiben. Es kann leer bleiben.

Wenn der Netzkonnektor zusätzliche TLS-Verbindungen nutzt, die der Netzkonnektor selbst managed, so werden diese vom obigen SFR nicht betroffen. Für solche Verbindungen soll der ST Autor deren Sicherheitsverhalten durch geeignete zusätzliche SFRs definieren. Dazu können neben oder statt von Managment-SFRs (Klasse MOT) auch SFRs zur Definition einer Informationsflußkontrollpolitik oder Zugriffskontrollpolitik genutzt werden.

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

Anwendungshinweis 108: Wenn es für den Hersteller des Netzkonnektors für die Dokumentation zu den Klassen ADV und ATE einfacher erscheint, das im SFR beschriebene Managment der TLS-Verbindungen ganz oder teilweise bereits beim Netzkonnektor anzusiedeln, soll dies ausdrücklich erlaubt sein. In diesem Sinne ist der letzte Satz im SFR zu verstehen. Insbesondere kann er auch einige oder alle auf TLS-Verbindungen bezogenen SFRs aus dem Schutzprofil für den Konnektor hier übernehmen.

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**

[125] refinement

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)

6.4.1. Abbildung der EVG-Ziele auf Sicherheitsanforderungen

Tabelle 5 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.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									
FTP_TRP.1/NK.Admin	X			X									
FMT_SMF.1/NK	X			X							X	X	
FMT_MSA.1/NK.PF				X							X	X	
FMT_MSA.4/NK				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			
FCS_CKM.4/NK	X	X	X				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.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.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 5: 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 6 jedes EVG-Ziel in einzelne Teilaspekte zerlegt, die dann auf Sicherheitsanforderungen abgebildet werden.[126] 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 Sicherheitsanforderungen (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 abhängige SFRs ebenfalls mit aufgelistet. Dabei wird davon ausgegangen, dass die Abhängigkeit selbst nicht gesondert erläutert werden muss.

[126] 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

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
O.NK.TLS_Krypto	TLS-Kanäle	FTP_ITC.1/NK.TLS FMT_MOF.1/NK.TLS FMT_SMR.1./NK FMT_SMF.1/NK FPT_TDC.1/NK.TLS.Zert
	Begründung: In O.NK.TLS_Krypto wird gefordert: *„Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung“* Genau dies leistet FTP_ITC.1/NK.TLS. Mit FMT_MOF.1/NK.TLS wird der Rolle Anwendungskonnektor die Möglichkeit gegeben die TLS-Verbindungen zu Managen und je nach Anwendungsfall einzurichten. FMT_SMF.1/NK definiert diese Funktionalität und FMT_SMR.1./NK definiert diese Rolle (Anwendungskonnektor). Zertifikate die im Rahmen von TLS-Verbindungen zum Einsatz kommen werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.	
	Kommunikation mit anderen IT-Produkten 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 FCS_COP.1/NK.TLS.AES FCS_COP.1/NK.TLS.Auth FCS_CKM.4/NK

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	Begründung: Für die TLS-Kanäle sind nach O.NK.TLS_Krypto nur „*sichere kryptographische Algorithmen und Protokolle gemäß [13] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [17]*“ 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, 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	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	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 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;	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	FCS_CKM.4/NK unterstützt als abhängige Komponenten dabei.	
O.NK.Admin_EVG	rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen Identifikation / Autorisierung des Administrators sicherer Pfad Beschränkung der Administration der Firewall-Regeln	FMT_MTD.1/NK FMT_SMR.1./NK FMT_SMF.1/NK FIA_UID.1/NK.SMR FMT_MSA.4/NK FTP_TRP.1/NK.Admin FMT_MSA.1/NK.PF
	Begründung: „*Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen.*“ → FMT_MTD.1/NK beschränkt den Zugriff wie vom Ziel gefordert auf die Rolle Administrator. FMT_SMR.1./NK modelliert als abhängige Komponente diese Rolle (Administrator). FIA_UID.1/NK.SMR erfordert eine Identifikation des Benutzers vor jeglichem Zugriff auf administrative Funktionalität. Die Menge der administrativen Funktionen wird in FMT_SMF.1/NK aufgelistet. „*Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung (auf Basis einer in der IT-Umgebung durchgeführten Authentisierung) eines Administrators, welcher die lokale und/oder (optional) entfernte Administration des EVG durchführen kann.*“ → Da die Authentisierung des Administrators in der Einsatzumgebung erfolgen kann, muss der EVG die Autorisierung als Sicherheitsattribut von außen übernehmen. Die dabei anzuwendenden Regeln wurden in FMT_MSA.4/NK modelliert. „*Die Administration erfolgt rollenbasiert.*“ → FMT_SMR.1./NK modelliert die Rolle Administrator. „*Weil die Administration über Netzverbindungen (lokal über PS2 oder zentral über PS3) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).*“ → FTP_TRP.1/NK.Admin fordert genau diesen sicheren logischen Kanal zum Benutzer (trusted path). „*Der EVG verhindert die Administration folgender Firewall-Regeln: ...*“ → Dieser Aspekt wird durch das Refinement zu FMT_MSA.1/NK.PF abgebildet. Schließlich unterstützt die Benutzerdokumentation (AGD_OPE.1) bei der Administration der Paketfilter-Regeln.	
O.NK.Protokoll	EVG protokolliert sicherheitsrelevante Ereignisse mit Daten und Zeitstempel	FAU_GEN.1/NK.SecLog FAU_GEN.2/NK.SecLog

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
		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.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	FPT_TDC.1/NK.Zert

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	mit Hilfe von TSL und der CRL	
	Begründung: Zertifikatsprüfung: „*Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form einer zugehörigen CRL und einer TSL bereitgestellt.*“ FPT_TDC.1/NK.Zert fordert, dass der EVG Informationen über die Gültigkeit von Zertifikaten korrekt interpretiert. In der Zuweisung wurden TSL und CRL explizit erwähnt: „*The TSF shall provide the capability to consistently interpret information – distributed in the form of a TSL (Trust-Service Status List) or CRL (Certificate Revocation List) information …*“ Die Zertifikatsprüfung wird für VPN-Konzentratoren der Telematikinfrastruktur-Netzes bzw. des Sicheren Internet Service durchgeführt. FPT_TDC.1/NK.Zert fordert ferner explizit, dass der EVG Informationen „*about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects”*interpretiert.	
O.NK.VPN_Vertraul	Vertraulichkeit der Nutzdaten im VPN (Telematikinfrastruktur-Netz) IPsec-Kanal: Ableitung von *session keys*, AES-Verschlüsselung mit den *session keys* , Zerstörung der *session keys* nach Verwendung, Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.IPsec, → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_COP.1/NK.ESP → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Vertraulichkeit der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der 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“).	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	FCS_COP.1/NK.IPsec ermöglicht die Definition der zu verwendenden Verschlüsselungsalgorithmen, hier AES gemäß FCS_COP.1/NK.ESP. FCS_CKM.4/NK unterstützt als abhängige Komponente ebenfalls. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet. FCS_CKM.1/NK fordert eine solche Generierung von *session keys*. *„Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.*“ → Mittels FCS_CKM.2/NK.IKE (IKE) werden die abgeleiteten Sitzungsschlüssel, die für die Verschlüsselung verwendet werden, mit der die Vertraulichkeit der Nutzdaten sichergestellt wird, mit der Gegenstelle ausgetauscht. Die Nutzdaten werden mit AES gemäß FCS_COP.1/NK.ESP verschlüsselt. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.VPN_Integrität	Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von *session keys*, Austausch der *session keys* mit Gegenstelle, Zerstörung der *session keys* nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von *session keys*, Zerstörung der *session keys* nach Verwendung Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Hash → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK FCS_COP.1/NK.HMAC → FCS_CKM.1/NK → FCS_CKM.4/NK FPT_EMS.1/NK
	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“).	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Encapsulating Security Payload (ESP) (RFC 4303 (ESP), [28]) 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 ([32], [33], [29]). 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 6.3)
	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: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.3)
	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 6: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 109: Hinweis zu O.NK.VPN_Integrität: Wird zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash eine Hashfunktion verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruht, sind keine geheimzuhaltenden Schlüssel erforderlich. Wird eine Hashfunktion verwendet, die auf einem symmetrischen Verschlüsselungsalgorithmus beruht, ergeben sich die üblichen Abhängigkeiten (FCS_CKM.1/NK, FCS_CKM.4/NK); in diesem Fall soll der ST-Autor diese Abhängigkeiten in Tabelle 5 aufnehmen und in Tabelle 6 (oben) begründen.

6.4.2. Erfüllung der Abhängigkeiten

6.4.2.1. Erfüllung der funktionalen Anforderungen

In Abschnitt 6.1 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 7 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 7: 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

Es waren keine Erweiterungen des CC Teil 3 [3] erforderlich.

Um die funktionalen Anforderungen an den EVG zu formulieren, war eine Erweiterung des CC Teil 2 [2] erforderlich: FPT_EMS.1/NK.

Die erweiterte Familie FPT_EMS ist im Abschnitt 5.1 definiert. Diese erweiterte Komponente wurde bereits im PP COS G2 [10], Abschnitt 6.6.1, definiert und motiviert. Die wichtigsten Argumente der Begründung werden im Folgenden wiedergegeben.

Die TSF soll Angriffe verhindern, die sich gegen vom EVG verarbeitete Geheimnisse richten, wobei die Angriffe extern beobachtbare physikalische Phänomene ausnutzen. Dies umfasst

neben anderen Geheimnissen insbesondere auch die Verwendung des privaten Authentisierungsschlüssels für die VPN-Tunnel (FTP_ITC.1/NK.VPN_TI). Der Schlüssel selbst wird bereits durch die gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG soll darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll verhindern, etwa die abgeleiteten Session Keys. Ein Beispiel für solche Angriffe sind Timing-Angriffe; für weitere Details siehe die Diskussion in Abschnitt 7.6.16. Die Familie FPT_EMS beschreibt die funktionalen Anforderungen an eine Beschränkung der ausnutzbaren Ausstrahlung über die Netzwerkschnittstellen.

6.6. Erklärung für die gewählte EAL-Stufe

Der Netzkonnektor (EVG) stellt die Verbindung zwischen den dezentralen Komponenten eines Leistungserbringers und der zentralen Telematikinfrastruktur-Plattform dar. Diese Verbindung wird unter Nutzung potentiell unsicherer Transportnetze hergestellt, z. B. über das Internet. Diese Tatsache macht den Netzkonnektor weltweit erreichbar und potentiell verwundbar. Der Netzkonnektor soll das lokale Netz des Leistungserbringers vom Transportnetz separieren. Da sich im lokalen Netz des Leistungserbringers sensitive, personenbezogene zu schützende Daten der TI *und der Bestandsnetze* befinden, muss davon ausgegangen werden, dass aus dem Transportnetz bzw. dem Internet Angriffe gegen den Netzkonnektor mit hohem Angriffspotential durchgeführt werden.

Damit die Evaluierung nachweisen kann, dass der Netzkonnektor diese Angriffe erfolgreich abwehrt, muss eine methodische Schwachstellenanalyse durchgeführt werden, die genau dieses hohe Angriffspotential berücksichtigt. Deshalb wurde AVA_VAN.5 ausgewählt. Eine so tiefgehende Schwachstellenanalyse ist für den Evaluator nur dann sinnvoll möglich, wenn hinreichend viele und detaillierte Informationen über den EVG zur Verfügung stehen. Dies spiegelt sich in den durch CC Teil 3 [3] für AVA_VAN.5 definierten Abhängigkeiten wider (insbesondere ADV_TDS.3 und ADV_IMP.1). Löst man alle Abhängigkeiten auf, so ergeben sich zusätzlich auch noch ALC_TAT.1 (als Abhängigkeit vom ADV_IMP.1) und ADV_FSP.4 (als Abhängigkeit von ADV_TDS.3); siehe auch Tabelle 7 in Abschnitt 6.4.2.2 oben.

Zieht man diese Komponenten in Betracht, so ergibt sich, dass nur eine Evaluierung nach einer sehr stark augmentierten Stufe EAL3+ oder nach der Stufe EAL4+ überhaupt in Frage kommen. In diesem Fall wurde schließlich zugunsten der Stufe EAL3+ entschieden.

Schließlich wurde die EAL-Stufe auch noch um ALC_FLR.2 erweitert. Der Hintergrund hierfür ist die Tatsache, dass Netzkonnektoren in großen Stückzahlen zum Einsatz kommen, an ein potentiell unsicheres Transportnetz (z. B. Internet) angeschlossen werden und während normaler Betriebszeiten üblicherweise im Online-Betrieb arbeiten. Es ist zu befürchten, dass im Laufe der Zeit Schwachstellen bekannt werden. Deren negative Auswirkungen sollen durch Prozeduren zur Fehlerbehebung begrenzt werden.

7. Anhang

7.1. 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 110: Der Anwendungskonnektor ist dafür verantwortlich, dass medizinische Daten, die vom EVG verarbeitet werden, bereits verschlüsselt sind, wenn sie an den EVG übergeben werden.

7.2. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AH	Authentication Header, siehe RFC 2402 und RFC 4302 [26]
AK	Anwendungskonnektor: Der Teil des Gesamtkonnektors, der nicht Netzkonnektor ist, wird als Anwendungskonnektor bezeichnet.
AK-PP	Schutzprofil (Protection Profile) für den Anwendungskonnektor
AVS	Apothekenverwaltungssystem
BA	Berufsausweis
Bestands-netz	Bestehende Netzwerke oder zukünftige sektorale Netze, die Anschluss an die TI erhalten sollen.
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (siehe www.bundesnetzagentur.de)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CAMS	Card Application Management System
CRL, CRLs	Certificate Revocation List(s)
CS	Clientsystem
DHCP	Dynamic Host Configuration Protocol: Protokoll, das die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server realisiert
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information (siehe www.dimdi.de) , eine nachgeordnete Behörde des Bundesministeriums für Gesundheit (BMG)
DoS	Denial of Service, übersetzt etwa Dienstverweigerung; bezeichnet einen Angriff auf einen Server mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen; in der Regel geschieht dies durch Überlastung
DRNG	Deterministic Random Number Generator deterministischer Zufallszahlengenerator (siehe [5])
DSL	Digital Subscriber Line
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card (englischer Begriff für eGK)
ESP	Encapsulating Security Payload; siehe RFC 2406 [27] bzw. zukünftig RFC 4303 [28]; für die jeweils zu verwendenden Standards siehe die Konnektorspezifikation [15]
gematik	gematik GmbH, siehe https://www.gematik.de/
GKV	gesetzliche Krankenversicherung

Abkürzung	Bedeutung
HBA	Heilberufsausweis
HPC	Health Professional Card (englischer Begriff für HBA)
HSM	High Security Modul, Hochsicherheitsmodul; sicherer Schlüsselspeicher mit der Möglichkeit, kryptographische Berechnungen auszuführen, ohne dass das Schlüsselmaterial das HSM verlässt
HSM-B	Eine HSM-Variante einer Institutionskarte Typ B (Secure Module Card). Das SM-B wird in dieser Fassung als virtuelle Karte verstanden, welches in einem virtuellen Kartenterminal steckt.
IAG	Internetzugangspunkt des Leistungserbringers
IKE	Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 [29]
IP	Internet Protocol
IPsec	IP Security, vgl. RFC 2401 bzw. RFC 4301 [25]
IPv4	Internet Protocol version 4, siehe RFC 791
IPv6	Internet Protocol version 6, siehe RFC 2460
KIS	Krankenhausinformationssystem
LE	Leistungserbringer
KV	Kassenärztliche Vereinigung
LAN	lokales Netzwerk (local area network), meist im Zusammenhang mit dem lokalen Netzwerk eines Leistungserbringers verwendet
LS*n*	logische Schnittstelle Nr. *n* (siehe Abschnitt 1.3.3.2)
MAC	Message Authentication Code; kryptographische Prüfsumme zum Schutz der Datenintegrität; vergleichbar einer Signatur, aber erstellt unter Verwendung eines symmetrischen Kryptoalgorithmus’
NAT	Network Address Translation, siehe RFC 2663
NK	Netzkonnektor, einer der Hauptfunktionsblöcke des Konnektors (siehe auch AK)
NTP	Network Time Protocol, siehe RFC 958 (Sept. 1985) und NTP Version 4 Release Notes (Okt. 2005)
OCSP	Online Certificate Status Protocol, siehe RFC 2560
PIN	Persönliche Identifikationsnummer, dient zur Authentisierung eines menschlichen Benutzers gegenüber einem IT-System (hier: gSMC-K)
PKV	private Krankenversicherung
PP	Protection Profile (Schutzprofil)
PS*n*	physische Schnittstelle Nr. *n* (siehe Abschnitt 1.3.3.1)
PVS	Praxisverwaltungssystem

Abkürzung	Bedeutung
RFC	Request for comment, siehe http://tools.ietf.org/html/
RSA	asymmetrisches Kryptoverfahren, benannt nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman
SAK	Bezeichnung einer Identität des Konnektors; steht für Signaturanwendungskomponente (einem Begriff aus dem Signaturgesetz)
SAR	Security Assurance Requirement Anforderung an die Vertrauenswürdigkeit des EVG
SFR	Security Functional Requirement funktionale Sicherheitsanforderung an den EVG
SGB V	Sozialgesetzbuch, fünftes Buch; dessen § 291a beschreibt die Einführung der elektronischen Gesundheitskarte
SICCT	Secure Interoperable Chip Card Terminal, Kartenleser
SIS	Sicherer Internet Service: Ein Internet-Zugangspunkt, der die damit verbundenen lokalen Netze und Systeme gegen Angriffe aus dem Internet schützt.
SM-B	Zusammenfassender Begriff für eine SMC-B (Institutionskarte Typ B), als auch eine in einem HSM-B (Hardware Security Module) enthaltene virtuelle SMC-B.
SMC	Security Module Card, Sicherheitsmodul (hier: Chipkarte als sicherer Schlüsselspeicher)
SMC-B	Security Module Card, Typ B, Träger der kryptographischen Identität der Institution des Leistungserbringers; wird u. a. vom AK zur Authentisierung gegenüber zentralen Diensten (Fachanwendungen) verwendet
gSMC-K	Geräte-Security Module Card Konnkektor: Sicherheitsmodul (für den) Netzkonnektor Bezeichnung für die Anwendung auf dem Sicherheitsmodul SM-K (oder einem der Sicherheitsmodule SM-K) des Einbox-Konnektors, welches das vom NK benötigte Schlüsselmaterial speichert. Träger der kryptographischen Identität des Netzkonnektors; wird insbesondere vom Netzkonnektor zur Authentisierung gegenüber dem VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform verwendet.
SM-K	Sicherheitsmodul für den Konnektor, kann z. B. in Form einer Chipkarte ausgeprägt sein; falls das SM-K die *Spezifikation der gSMC-K* / Objektsystem [19] erfüllt, wird es als SMC-K bezeichnet
SM-K-PP	Schutzprofil für das Sicherheitsmodul für den Konnektor, vgl. *Card Operating System (PP COS)* [10]
SM-KT	Sicherheitsmodul für das Kartenterminal
SM-SAK	Sicherheitsmodul (für die) Signaturanwendungskomponente (SAK) des

Abkürzung	Bedeutung
	Konnektors Bezeichnung für die Anwendung auf dem Sicherheitsmodul SM-K (oder einem der Sicherheitsmodule SM-K) des Einbox-Konnektors, welches das von der Signaturanwendung benötigte Schlüsselmaterial speichert.
SNTP	Simple Network Time Protocol, siehe RFC 4330
SSCD	Secure Signature Creation Device, englisches Pendant zu SSEE
SSEE	Sichere Signaturerstellungseinheit, deutsches Pendant zu SSCD
SSL	Secure Sockets Layer, Kommunikationsprotokoll ersetzt durch TLS.
ST	Security Target
ST-Autor	Autor des Security Targets (welches basierend auf diesem PP erstellt wird)
TCP	Transmission Control Protocol, siehe RFC 793 und RFC 1323
TLS	Transport Layer Security
EVG	Target of evaluation; (deutsches Synonym: Evaluationsgegenstand, abgekürzt: EVG)
TSF	EVG Security Functionality (Definition aus CC v3.1 R5, Teil 1 [1]: „combined functionality of all hardware, software, and firmware of a EVG that must be relied upon for the correct enforcement of the SFRs”
TSL	Trust-Service Status List, siehe Glossar, Kapitel 7.3
USB	Universal Serial Bus
VODD	Verordnungsdaten-Dienst; zentraler Dienst zur Verwaltung von Verordnungen (umgangssprachlich: „Rezepten“)
VPN	virtuelles (nur logisch getrennt existierendes) privates Netz (virtual private network) Ein VPN nutzt ein offenes, ungeschütztes Netz (z. B. das Internet) als Transportmedium und ermöglicht darauf eine gesicherte Verbindung zwischen den rechtmäßigen Teilnehmern des VPNs, die sich durch den Besitz kryptographischer Schlüssel als solche ausweisen. Die in einem VPN übertragenen Daten werden in aller Regel durch Verschlüsselung gegen unbefugte Kenntnisnahme und durch kryptographische Prüfsummen gegen unbemerkte Veränderung geschützt.
VPN-TI	VPN-Konzentrator für den Zugriff auf die zentrale Telematikinfrastruktur-Plattform
VPN-SIS	VPN-Konzentrator für den Zugriff auf den Internet-Zugangspunkt (SIS)
VSD	Versicherten-Stammdaten
VSDD	Versicherten-Stammdaten-Dienst (zentraler Dienst)
WAN	Weitverkehrsnetzwerk (wide area network), meist im für das Transportnetz zur Anbindung der Leistungserbringer an die zentrale Telematikinfrastruktur-

Abkürzung	Bedeutung
	Plattform verwendet; beispielsweise kann das Internet als Transportmedium für ein VPN genutzt werden
X.509	Standard der ITU-T (International Telecommunication Union) für Public Key Infrastrukturen und insbesondere für den Aufbau von Zertifikaten

Tabelle 8: Abkürzungsverzeichnis

7.3. Glossar

Begriff	Bedeutung
application connector	Anwendungskonnektor
Attacker	Angreifer (siehe auch Abschnitt 3.2)
Bestandsnetze	Bestehende Netzwerke, die (zukünftig) Anschluss an die TI erhalten sollen.
Box	Der Begriff Box wird im Zusammenhang mit den Begriffen „Einbox-Konnektor“ bzw. „Einboxlösung“ und „Mehrkomponentenlösung“ bzw. „Mehrkomponenten-Konnektor“ verwendet. Die „Box“ bezeichnet dabei ein gemeinsames Gehäuse. Wenn eine Einboxlösung in sicherer Umgebung steht (was sie gemäß der Annahme A.phys_Schutz tut), dann kann es keine Angriffe auf die interne Kommunikation zwischen den Konnektorteilen (NK, AK, gSMC-K) geben. Im Fall einer Mehrboxlösung werden Angriffe auf die Kommunikation zwischen den Konnektorteilen betrachtet. Diese Angriffe müssen dann entweder technisch (z. B. durch gegenseitige Authentisierung und den Aufbau eines sicheren Kanals) oder organisatorisch abgewehrt werden.
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 im Konnektor, die die Anwendungslogik der Fachanwendungen im Konnektor umsetzen und

Begriff	Bedeutung
(Fachmodule)	(Sicherheits-)Funktionen des Konnektors nutzen
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*

Begriff	Bedeutung
	Telematiksicherheitsrichtlinien erfüllen. Ohne diese spezielle Infrastruktur beim Leistungserbringer ist es nicht möglich, einen Kommunikationskanal in die Telematikinfrastruktur aufzubauen. […]“

Tabelle 9: Glossar

7.4. Abbildungsverzeichnis

7.5. Tabellenverzeichnis

7.6. Anwendungshinweise (Application Notes) für den Autor der Sicherheitsvorgaben (Security Target)

Dieser Abschnitt enthält weitere Hinweise für den ST-Autor zur Verwendung des Schutzprofils, die nicht in Form vom Application Notes im Fließtext gegeben wurden, um den Lesefluss nicht zu stören.

7.6.1. Sperrung kryptographischer Identitäten

Technisch besteht grundsätzlich die Möglichkeit, einzelne (z. B. gestohlen gemeldete) EVGs oder auch ganze Baureihen von EVGs zu sperren (z. B. bei Bekanntwerden eines Problems, welches eine gesamte Baureihe betrifft), indem die entsprechenden Zertifikate gesperrt bzw.

zurückgerufen werden. Solche Aspekte liegen außerhalb dieses Schutzprofils und müssen in einem Betriebskonzept adressiert werden.

7.6.2. Bösartige Software im LAN (zu Abschnitt 1.3.2 und zu Abschnitt 3.5, A.NK.CS)

Obwohl das Vorhandensein bösartiger Software auf IT-Systemen im LAN durch die Annahme A.NK.Betrieb_CS verhindert werden soll, muss nach dem Stand der Technik davon ausgegangen werden, dass Leistungserbringer eine Kompromittierung eines ihrer IT-Systeme im LAN nicht sicher verhindern bzw. nicht in jedem Fall frühzeitig erkennen können. Dieses Schutzprofil betrachtet daher auch Angriffe aus dem LAN heraus gegen den Netzkonnektor (an seiner LAN-seitigen Schnittstelle), siehe dazu die Bedrohungen T.NK.local_EVG_LAN und T.NK.remote_EVG_LAN in den Abschnitten 3.3.2.1 und 3.3.2.3 sowie die Ausführungen zu Leistungserbringern in Abschnitt 3.2.1.

7.6.3. Der Konnektor als Mehrkomponenten-Lösung

Das vorliegende Schutzprofil formuliert Sicherheitsanforderungen an einen Einbox-Konnektor (Einboxlösung) und in Abbildung 2 in Abschnitt 1.3.2 ist der Fall einer Einboxlösung für den Konnektor dargestellt. Es ist grundsätzlich nicht ausgeschlossen, Anwendungskonnektor und Netzkonnektor auf mehrere physische Einheiten zu verteilen bzw. als getrennte Produkte in jeweils eigenem Gehäuse zu gestalten und dennoch in Anlehnung an dieses Schutzprofil zu evaluieren. Für Hersteller, die dieses Schutzprofil als Grundlage für ein Security Target einer Mehrkomponenten-Lösung verwenden wollen, werden im folgenden einige Hinweise gegeben.

Teilt ein Hersteller seinen Konnektor physisch auf mehrere Boxen auf und will er einen solchen Mehrkomponenten-Konnektor in Anlehnung an dieses Schutzprofil evaluieren, so muss er organisatorische oder technische Anforderungen für eine sichere Kommunikation zwischen den getrennten Teilen formulieren.

Organisatorischer Schutz kann beispielsweise dadurch erreicht werden, dass Anwendungskonnektor und Netzkonnektor im selben zutrittsgeschützten Serverraum bzw. Rechenzentrum einer Klinik aufgestellt werden.

Technischer Schutz kann durch kryptographische Sicherung der Kommunikation implementiert werden, beispielsweise durch einen TLS-Kanal mit vorausgehender gegenseitiger Authentisierung.

Wird ein solcher sicherer Kanal kryptographisch implementiert, so ist ein geeignetes Schlüsselmanagement erforderlich (Schlüsselvereinbarung bzw. –austausch, sichere Schlüsselspeicherung).

Abhängig von der Ausgestaltung des Konnektors ist ein sicherer Kanal zwischen Netzkonnektor und Anwendungskonnektor zu etablieren. Die Forderung nach einem sicheren Kanal zwischen Netzkonnektor und Anwendungskonnektor kann bei einer Einbox-Lösung entfallen (siehe auch Abschnitt 7.6.3 und Abschnitt 7.6.15).

Es steht dem ST-Autor frei, die Anforderungen an die Einsatzumgebung in A.NK.phys_Schutz und OE.NK.phys_Schutz abzuschwächen, indem der Schutz des Kommunikationskanals zwischen Konnektorteilen aus A.NK.phys_Schutz und OE.NK.phys_Schutz herausgenommen wird und dieser Aspekt des Umgebungsziels OE.NK.phys_Schutz in ein Ziel für den EVG umgewandelt wird.

Der ST-Autor soll die Einsatzumgebung des Netzkonnektors in seiner konkreten Ausprägung beschreiben.

Die Einsatzumgebung des Konnektors im allgemeinsten Fall (Mehrkomponenten-Lösung) ist in der folgenden Abbildung 4 dargestellt. Zum Verständnis der Abbildung 4 siehe auch die Hinweise zu Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung) in Abschnitt 1.3.2 Einsatzumgebung des Konnektors sowie das Abkürzungsverzeichnis in Abschnitt 7.2.

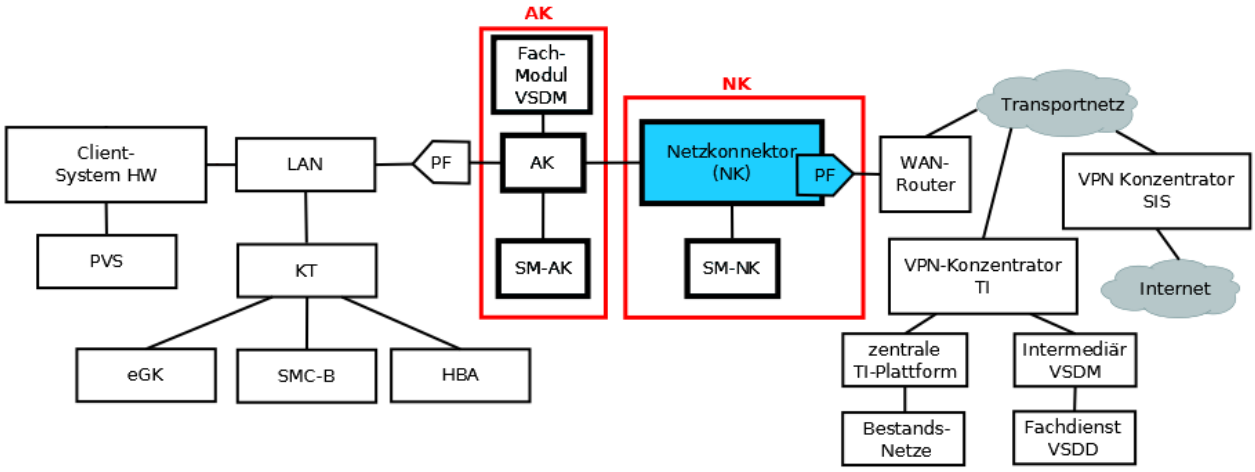

Abbildung 4: Einsatzumgebung des Konnektors, Mehrkomponenten-Lösung
(ein zusätzlicher Paketfilter schützt den AK)

Auch im Fall einer Mehrkomponenten-Lösung muss der Anwendungskonnektor vor Angriffen aus dem LAN geschützt werden. Dieser Schutz muss aber nicht durch den Netzkonnektor geleistet werden. Falls der Netzkonnektor dies nicht leistet, muss eine zusätzliche Komponente eingesetzt werden, welche gleichwertige Sicherheit bietet (siehe Abschnitt 7.6.17). In Abbildung 4 wird diese Komponente mit dem Begriff „Paketfilter“ bezeichnet.

Bei der hier als Mehrkomponenten-Lösung bezeichneten Variante handelt es sich um eine typische Lösung für Krankenhäuser mit eigenem Rechenzentrum: Netzkonnektor und Anwendungskonnektor sind als reine Software-Lösung realisiert und laufen auf Servern im Rechenzentrum ab.

Der ST-Autor muss im Security Target die Einsatzumgebung eindeutig beschreiben. Er sollte dazu eine Skizze erstellen, vergleichbar zu Abbildung 4. Die Skizze muss geeignet sein, die physischen und logischen Schnittstellen zwischen dem EVG und seiner IT-Umgebung zu erkennen. Abhängig von der konkreten Ausprägung des Produkts ist die Beschreibung der Schnittstellen in Abschnitt 1.3.3 geeignet anzupassen.

7.6.4. Aufbau und physische Abgrenzung des Netzkonnektors (zu Abschnitt 1.3.4)

Zuordnung der Basisdienste zu Konnektorteilen: Bei einer Realisierung des Konnektors als Mehrkomponenten-Lösung (siehe auch Abschnitt 7.6.3) soll der ST-Autor beschreiben, welche einzelne Bestandteile des Konnektors ggf. mehrfach vorhanden sind und/oder welche Dienste durch mehrere Konnektorteile gemeinsam genutzt werden.

Beispiel: Der Netzkonnektor verfügt grundsätzlich über die Fähigkeit, kryptographische Operationen durchzuführen (dies stellt einen Basisdienst dar). Kryptographische Funktionalität kann in einer kryptographischen Funktionsbibliothek gebündelt sein und diese kann auch von mehreren Konnektorteilen gemeinsam genutzt werden. Der ST-Autor soll beschreiben, ob und ggf. welche gemeinsam genutzten Komponenten es gibt.

Der ST-Autor soll den EVG physisch exakt abgrenzen. Um die Menge möglicher Implementierungen nicht einzuschränken, werden in diesem Schutzprofil bewusst wenig Einschränkungen formuliert. Die im Security Target vorgenommene Abgrenzung muss so eindeutig sein, dass für jede Komponente entscheidbar ist, ob sie Teil des EVGs ist oder nicht.

Der Netzkonnektor kann sowohl als reine Software-Lösung implementiert werden als auch in Form einer aus Hardware und Software bestehenden Box.

Reine Software-Lösungen: Realisierungen eines Konnektors als reine Software-Lösungen sind grundsätzlich denkbar, beispielsweise „begehbare Konnektoren“ in Form eines Serverraums in einem Krankenhaus. In jedem Fall muss die Umgebung des Konnektors für physische Sicherheit sorgen (vor phyischem Zugriff geschützter Bereich, siehe A.NK.phys_Schutz). Die Nutzung eines Sicherheitsmoduls (gSMC-K, beispielsweise in einer Ausprägung als Chipkarte oder als Hochsicherheitsmodul (HSM)) zum Nachweis der Bauartzulassung ist auch in diesem Fall erforderlich. Die Implementierung des Netzkonnektors muss aber hinreichend resistent gegen Angriffe sein (AVA_VAN.5) und zum Nachladen von ausführbarem Code muss eine hinreichend strenge Separation vom EVG durchgesetzt werden.

Im Falle einer aus Hardware und Software bestehenden Lösung kann der Konnektor sich physisch über mehrere Gehäuse verteilen (Mehrkomponenten-Lösung) oder Anwendungskonnektor und Netzkonnektor können im selben Gehäuse vereint sein (Einbox-Lösung). Gleiches gilt sinngemäß für reine Software-Lösungen: Die Funktionalitäten von Anwendungskonnektor und Netzkonnektor können in einem Programm-Modul vereint oder über mehrere Module verteilt sein. Siehe dazu auch Abschnitt 7.6.3 Der Konnektor als Mehrkomponenten-Lösung und Zuordnung der Basisdienste zu Konnektorteilen (weiter oben).

Der EVG wird für einen spezifischen Einsatzzweck entwickelt. Dies schließt aber nicht aus, dass vorgefertigte Komponenten (z. B. PC-Hardware und –Software) als Teil des EVG verwendet werden. Es steht dem ST-Autor frei, bei der Definition des EVGs beispielsweise ein Betriebssystem oder Teile des Betriebssystems zum Bestandteil des EVGs zu erklären. Es ist jedoch zwingend erforderlich, dass die in diesem Schutzprofil geforderte Sicherheitsfunktionalität vom EVG erbracht wird. Es ist beispielsweise nicht zulässig, Sicherheitsfunktionalität des Betriebssystems zu nutzen, ohne dass diese evaluiert wird. Als einzige Ausnahme zu dieser Regel können gewisse komplexe Mechanismen von

Betriebssystemen, welche vom Netzkonnektor verwendete Sicherheitsfunktionalität umsetzen (z. B. Separationsmechanismen, wie der protected mode eines Intel-kompatiblen Prozessors, eine Prozesstrennung unter Unix oder Application Firewalls in Java), dem Netzkonnektor als (nicht zu evaluierende) IT-Einsatzumgebung zur Verfügung gestellt werden; siehe dazu auch die Diskussion „Betriebssystem als Bestandteil des EVG oder der Umgebung“ in Abschnitt 7.6.5.

Bei der Abgrenzung des EVGs soll der ST-Autor auch berücksichtigen, ob der Benutzer des EVGs die Möglichkeit besitzt, die getroffenen Annahmen an die IT-Einsatzumgebung zu erfüllen.

Zusätzlicher ausführbarer Code auf dem Netzkonnektor: Unter zusätzlichem Code wird Code verstanden, der Funktionalität implementiert, die über die Sicherheitsfunktionalität des Netzkonnektors hinausgeht, beispielsweise der Anwendungskonnektor. Dieses Schutzprofil geht von dem Standardfall aus, dass kein zusätzlicher ausführbarer Code auf dem Netzkonnektor abläuft. Falls zusätzlicher Code auf dem Netzkonnektor vorhanden ist, muss der ST-Autor festlegen, ob dieser Code Teil des EVG ist oder nicht. In jedem Fall gilt: Soll zusätzlicher ausführbarer Code auf dem Netzkonnektor ablaufen, so muss sichergestellt werden, dass dieser zusätzliche Code die Sicherheitsfunktionalität des EVGs nicht beeinträchtigt.

Sofern der zusätzliche Code zum Evaluierungszeitpunkt bereits bekannt ist, kann seine Unschädlichkeit im Rahmen der Evaluierung überprüft werden. Der Code kann dann nach der Zertifizierung nicht mehr verändert werden, ohne den zertifizierten Status des Netzkonnektors zu verlieren.

Sofern der Code zum Evaluierungszeitpunkt noch nicht bekannt ist oder gar die Möglichkeit zur Aktualisierung solchen Codes gegeben sein soll, muss der EVG über entsprechende Separationsmechanismen verfügen. Durch die Separationsmechanismen muss sichergestellt werden, dass Störungen der evaluierten Funktionalität des Netzkonnektors ausgeschlossen sind und dass allen durch den Anwendungskonnektor entstehenden Bedrohungen wirksam begegnet wird.

Der Hersteller des EVGs soll eine klare Aussage in das Security Target aufnehmen, ob zusätzlicher ausführbarer Code auf dem Konnektor vorhanden bzw. zulässig ist und ob Separationsmechanismen im Rahmen der Evaluierung untersucht werden sollen. In diesem Fall sind ein geeignetes Sicherheitsziel für den EVG sowie entsprechende funktionale Anforderungen zu ergänzen. Das Sicherheitsziel wiederum muss von einer Bedrohung (z. B.: Fehler in anderer Software-Komponente) oder einer organisatorischen Sicherheitspolitik (z. B.: es soll weitere Software auf der Plattform ablaufen können, auf der der Konnektor implementiert ist) abgeleitet werden.

Benutzerschnittstellen: Der Konnektor kann physische Benutzerschnittstellen (Tastatur) implementieren, er muss dies aber nicht tun. Die Kommunikation mit dem Benutzer kann über weitere dezentrale Komponenten vermittelt erfolgen. Der EVG kann für Benutzereingaben (z. B. Eingabe des Administrator-Passworts) externe IT-Systeme, beispielsweise die Tastatur und Anzeige von Kartenterminals oder von vertrauenswürdigen Clientsystemen, nutzen. Der ST-Autor muss darauf achten, dass die Vertrauenswürdigkeit der als Benutzerschnittstelle verwendeten IT-Systeme im Security Target gefordert wird und dass

die Kommunikationsflüsse – abhängig von den Annahmen an die Einsatzumgebung – falls erforderlich geeignet abgesichert werden.

Ausgabe von Zustandsmeldungen: Wenn der EVG über ein Display verfügt, müssen darüber auch sicherheitskritische Zustandsmeldungen ausgegeben werden.

Schutz von Authentisierungsgeheimnissen: Wenn der EVG die Eingabe von Authentisierungsgeheimnissen unterstützt (z. B. Eingabe des Administrator-Passworts), muss er diese Geheimnisse geeignet schützen. Der ST-Autor soll in diesem Fall ein entsprechendes EVG-Ziel in das Security Target aufnehmen oder O.NK.Schutz geeignet erweitern.

7.6.5. Betriebssystem als Bestandteil des EVG oder der Umgebung (zu Abschnitt 1.3.4)

Wenn das Betriebssystem Sicherheitsfunktionalität umsetzt, sind folgende Möglichkeiten denkbar:

Das gesamte Betriebssystem wird als Teil des EVG deklariert. Dies erfordert, dass das gesamte Betriebssystem untersucht werden muss und dass diese Untersuchung des Betriebssystems bei Aktualisierungen (Updates, Einspielen von Patches, o. ä.) des Betriebssystems wiederholt werden muss (das Einspielen eines Betriebssystem-Patches führt im Allgemeinen zum Verlust des Zertifikats für den Konnektor). Der gesamte Quellcode des Betriebssystems muss zur Prüfung vorgelegt werden; dies setzt also die Mitwirkung des Betriebssystem-Herstellers oder ein Open Source-Betriebssystem voraus. Die Nutzung bereits evaluierter und zertifizierter Betriebssysteme verspricht nur dann Vorteile, wenn auch genau die gewünschte Sicherheitsfunktionalität evaluiert wurde.

Diejenigen sicherheitsrelevanten Teile des Betriebssystems, welche vom Netzkonnektor verwendete Sicherheitsfunktionalität umsetzen (z. B. TCP/IP-Stack), werden als Teile des EVGs deklariert. Ein solches Vorgehen setzt voraus, dass entscheidbar ist, in welchen Teilen des Betriebssystems die Sicherheitsfunktionalität implementiert ist. Die sicherheitsrelevanten Teile des Quellcodes des Betriebssystems müssen zur Prüfung vorgelegt werden. Wiederholungen der Evaluierung des Betriebssystems (bzw. seiner Teile) sind nur noch dann erforderlich, wenn Aktualisierungen von sicherheitsrelevanten Teilen vorgenommen werden. Ob dieses Vorgehen praktikabel ist, hängt davon ab, wie oft Aktualisierungen erforderlich werden, wie gut die sicherheitsrelevanten Teile separiert werden können und wie gut die Auswirkungen von Patches auf die Sicherheitsfunktionalität analysierbar sind.

Gewisse komplexe Mechanismen von Betriebssystemen, welche vom Netzkonnektor verwendete Sicherheitsfunktionalität umsetzen (z. B. Separationsmechanismen, wie Prozesstrennung unter Unix oder Application Firewalls in Java), können dem Netzkonnektor als (nicht zu evaluierende) IT-Einsatzumgebung zur Verfügung gestellt werden. Üblicherweise sind diese komplexen Mechanismen über Jahre gereift, erprobt und oftmals eigenständig evaluiert. Das Erfordernis der Evaluierung solcher Mechanismen ist mit der Zertifizierungsstelle abzustimmen.

Die Sicherheitsfunktionalität wird vollständig in der Anwendungssoftware des Netzkonnektors implementiert. Unter Umständen ist es dabei erforderlich, bereits im Betriebssystem vorhandene Funktionalität (z. B. TCP/IP-Stack) erneut zu implementieren.

Wenn die Anwendungssoftware ihre Sicherheitsleistung unabhängig vom Betriebssystem erbringen kann, sind Aktualisierungen der Betriebssystem-Software unschädlich für die Gültigkeit des Common Criteria-Zertifikats des Netzkonnektors.

Zu beachten ist, dass üblicherweise im Rahmen der EVG-Prüfung das Betriebssystem mindestens[127] als IT-Einsatzumgebung mit getestet wird. Im Regelfall wird das Betriebssystem, auf dem der EVG getestet wurde, im Zertifikat benannt. Es ist im Einzelfall mit der Zertifizierungsstelle abzustimmen, wie sich Veränderungen des Betriebssystems auf die Gültigkeit des Zertifikats auswirken.

Bei der Abgrenzung des EVGs soll der ST-Autor auch berücksichtigen, ob der Benutzer des EVGs die Möglichkeit besitzt, die getroffenen Annahmen an die IT-Einsatzumgebung zu erfüllen.

Wird der EVG z. B. gemeinsam mit einem Betriebssystem ausgeliefert, auf dessen sichere Konfiguration der Anwender keinen Einfluss hat, erscheint es sinnvoll, diese Konfiguration des Betriebssystems im Rahmen der Evaluierung zu betrachten.

Wird der EVG hingegen auf dem vorhandenen Betriebssystem des Benutzers installiert, liegt dessen sichere Konfiguration in der Verantwortung des Benutzers. Es stellt sich dann jedoch die Frage, ob der Benutzer in der Lage ist, diese Verantwortung wahrzunehmen.

7.6.6. Gemeinsame Nutzung kryptographischer Funktionen (zu Abschnitt 1.3.5)

Es ist denkbar, dass kryptographische Funktionen des Netzkonnektors als Basisdienste auch nach außen zur Verfügung gestellt werden, z. B. zur Nutzung durch den Anwendungskonnektor oder durch die Clientsysteme.

Es wäre theoretisch auch denkbar, dass kryptographische Funktionen vom Anwendungskonnektor bereitgestellt und vom Netzkonnektor genutzt werden. Dieses Schutzprofil fordert jedoch, dass die kryptographischen Funktionen als Sicherheitsfunktionen des Netzkonnektors evaluiert werden. Im Falle einer Mehrkomponenten-Lösung ist es daher nicht zulässig, einen Netzkonnektor zu evaluieren, ohne dessen kryptographische Funktionalität im Rahmen der Evaluierung ebenfalls zu untersuchen. Es darf nicht auf eine zukünftige Evaluierung des Anwendungskonnektors verwiesen werden, höchstens auf eine bereits abgeschlossene. Denkbar sind Composite-Evaluierungen, bei denen ein Konnektor-Funktionsblock bereits evaluierte Funktionalität eines anderen Konnektor-Funktionsblocks nutzt; in diesem Fall umfasst der Composite-EVG beide Funktionsblöcke (Anwendungskonnektor und Netzkonnektor).

7.6.7. Physischer Schutz und EVG-Integritätsprüfung (zu Abschnitt 3.5 Annahmen, A.NK.phys_Schutz, zu Abschnitt 4.1.1, O.NK.Schutz und zu Abschnitt 4.2, OE.NK.phys_Schutz)

Das Schutzprofil geht davon aus (A.NK.phys_Schutz), dass die Einsatzumgebung physische Angriffe auf den Konnektor während seiner aktiven Nutzung abwehrt und das außerhalb und

[127] Das Betriebssystem (oder Teile des Betriebssystems) ist/sind entweder Teil des EVGs oder Bestandteil der IT-Einsatzumgebung. In diesem Sinne stellt das Betriebssystem „mindestens“ die IT-Einsatzumgebung dar.

vor seiner aktiven Nutzung Diebstahl und/oder physische Manipulation des Konnektors erkannt werden.

Aufgrund der Annahme A.NK.phys_Schutz muss der EVG selbst keinen Schutz gegen physische Manipulationen bieten. Daher wurde keine Anforderung aus der Familie FPT_PHP ausgewählt. Es steht dem ST-Autor aber frei, das Umgebungsziel OE.NK.phys_Schutz in ein Ziel für den EVG umzuwandeln (als neues Ziel oder Ergänzung eines bestehenden Ziels, z. B. zu O.NK.Schutz) und eine entsprechende Anforderung (z. B. aus der Familie FPT_PHP) an den EVG zu formulieren. Die Erfüllung dieser Anforderung muss dann jedoch gegen das betrachtete Angriffspotential (hoch) geprüft werden.

Die Gebrauchsanweisung beschreibt die Anforderungen zum physischen Schutz des Konnektors in der Einsatzumgebung (s. OE.NK.phys_Schutz) und gibt Sicherheitshinweise.

Das von O.NK.Schutz geforderte Erkennen bzw. Erkennbarmachen sicherheitstechnischer Veränderungen umfasst mindestens Versuche, den ausführbaren Code zu verändern. Selbsttests sollten bei jedem Start (Booten) die Integrität der installierten Images prüfen und bei Bedarf aufgerufen werden können. Der ST-Autor soll erklären, wie der EVG sich verhält und gegebenenfalls abweichendes Verhalten begründen.

Der ST-Autor soll beschreiben, wie der EVG seine Integrität überprüft und ob er ggf. auch die Integrität weiterer Komponenten prüft (z. B. zugrundeliegendes Betriebssystem). Falls ein Betriebssystem Sicherheitsfunktionalität umsetzt, gehören zumindest die umsetzenden Teile des Betriebssystems mit zum EVG und ihre Integrität ist dann ebenfalls zu sichern. Siehe auch Abschnitt 7.6.5 Betriebssystem als Bestandteil des EVG oder der Umgebung.

Falls die Integritätsprüfung kryptographisch abläuft, soll der ST-Autor außerdem beschreiben, welche kryptographischen Verfahren verwendet werden, welche Schlüssel verwendet werden und wo diese Schlüssel gespeichert werden. Ferner ist zu diskutieren, welche Maßnahmen getroffen wurden um zu verhindern, dass ein Angreifer die Selbsttest-Funktion deaktiviert bzw. manipuliert (beispielsweise Unterbringung des Prüfalgorithmus in einem nicht wiederbeschreibbaren Speicherbereich). Es ist zu beschreiben, wie auch im Fall von Software-Aktualisierung die Integrität des EVG sichergestellt werden kann.

Trotz der Annahme A.NK.phys_Schutz sind Angriffe an der logischen WAN-Schnittstelle auf die im EVG gespeicherten Geheimnisse denkbar. Aus diesem Grund enthält das Schutzprofil die Anforderung FPT_EMS.1/NK.

Da zum Zeitpunkt der Evaluierung des Produkts (Netzkonnektor) dessen spätere Einsatzumgebung noch nicht bekannt sein wird, wird die Evaluierung stets als Produkt-Evaluierung und nicht als System-Evaluierung[128] durchgeführt werden. Dies impliziert, dass die Erfüllung der Annahmen an die Einsatzumgebung nicht an einem (bzw. jedem) konkreten Einsatzort des EVGs überprüft wird.

[128] Ein „IT-System“ bezeichnet eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung.

7.6.8. Denial of Service Angriffe (zu Abschnitt 3.5 Annahmen, A.NK.kein_DoS, und Abschnitt 4.1.3 Ziele für die Paketfilter-Funktionalität, O.NK.PF_LAN)

Durch die explizite Erwähnung des Umgebungsziels OE.NK.kein_DoS wird deutlich abgegrenzt, welche Leistungen der EVG nicht erbringen kann bzw. wo er nur unterstützend tätig werden kann.

Der EVG besitzt kaum Möglichkeiten Denial of Service Angriffe abzuwehren. 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. Insofern kann der Netzkonnektor die Abwehr von Denial of Service Angriffen unterstützen, aber nicht die alleinige Verantwortung dafür übernehmen.

Der EVG kann dazu beitragen, Denial of Service Angriffe gegen die zentrale Telematikinfrastruktur-Plattform zu erschweren, indem sein LAN-seitiger Paketfilter Anfragen aus dem LAN filtert (dadurch können z. B. die Auswirkungen von Schadsoftware im LAN begrenzt werden) und nur aus Sicht des EVG zulässige Anfragen über den VPN-Tunnel an die zentrale Telematikinfrastruktur-Plattform gerichtet werden. Zulässige Anfragen an den EVG müssen vom Anwendungskonnektor stammen und wurden dann bereits dort plausibilisiert (z. B. XML-Schema-Prüfung). Der Anwendungskonnektor ist nicht Gegenstand dieses Schutzprofils.

Letztlich liegt die Verantwortung für den Schutz der Systeme der zentralen Telematik-infrastruktur-Plattform jedoch 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.

7.6.9. Korrekte Nutzung des Netzkonnektors (zu Abschnitt 3.5 Annahmen, A.NK.CS)

Das Schutzprofil schließt nicht aus, dass auf einem IT-System im LAN auch bösartiger Code abläuft (z. B. Trojaner). Der Konnektor muss sich daher gegen Angriffe aus dem Primärnetz ebenfalls schützen (siehe auch die Bedrohungen T.NK.local_EVG_LAN und Anwendungshinweis 18). Es muss aber, wie unter **A.NK.CS** formuliert, angenommen werden, dass die Clientsysteme die Dienste des Netzkonnektors korrekt aufrufen, da andernfalls der Konnektor nicht unterscheiden kann, welche Daten mittels VPN übertragen werden sollen (zu schützende Daten der TI *und der Bestandsnetze*, z. B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur-Plattform) und welche nicht.

Es wird angenommen, dass der Anwendungskonnektor die Dokumententypen der Dienste nach § 291 a SGB V [9] (z. B. eVerordnung) korrekt erkennt und unterscheiden kann (technisch wird dies durch Aufruf geeigneter Schnittstellen des Anwendungskonnektors umgesetzt) und auf dieser Basis den Netzkonnektor mit geeigneten Parametern aufruft. Siehe auch Abschnitt 7.6.14.

7.6.10. Sichere Administration des EVGs (zu Abschnitt 3.5, A.NK.Admin_EVG)

Das Recht zur Administration des EVG impliziert die Pflicht, den EVG in sicherer Weise zu administrieren. Das gilt z. B. für das Einstellen von Paketfilter-Filterregeln, falls der EVG

diese Möglichkeit bietet. Der ST-Autor soll beschreiben, welche Management-Funktionen (im Sinne der Klasse FMT, siehe Common Criteria, Teil 2 [2]) der EVG bietet.

7.6.11. Authentizität des Netzkonnektors (zu Abschnitt 4.1.1, O.NK.EVG_Authenticity)

Der ST-Autor soll beschreiben, wie die Authentizität des Netzkonnektors bei seiner Auslieferung gegenüber dem empfangenden Leistungserbringer oder dem von ihm beauftragten Servicetechniker nachgewiesen werden kann.

Einen hinreichenden Schutz gegen Angreifer, welche gefälschte Konnektoren in Umlauf bringen, stellen ein geeignetes Auslieferungsverfahren (ALC_DEL.1) sowie sichere Verfahren zur Inbetriebnahme (AGD_OPE.1) dar, sofern sie mit weiteren Maßnahmen kombiniert werden, welche spätere Veränderungen am Konnektor mit Sicherheit ausschließen oder hinreichend erkennbar machen, z. B. Aufbewahrung in einem gesicherten Bereich (siehe OE.NK.phys_Schutz).

Der Netzkonnektor muss auf Anforderung seine Authentizität nachweisen, indem er beispielsweise ein sicheres Authentisierungsprotokoll implementiert. Das dafür erforderliche Geheimnis kann er der gSMC-K entnehmen. Die Authentizität kann auch dadurch nachgewiesen werden, 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.

7.6.12. Externer Zufallszahlengenerator (zu Abschnitt 4.2 Sicherheitsziele für die Umgebung, OE.NK.RNG)

Der externe Zufallszahlengenerator kann beispielsweise durch das Sicherheitsmodul gSMC-K zur Verfügung gestellt werden – dies ist eine naheliegende Lösung.

Der Zufallszahlengenerator kann theoretisch auch durch ein SM-K realisiert werden. Falls die Zufallszahlen für den Netzkonnektor von einer dem Anwendungskonnektor zugeordneten SM-K bezogen werden, muss dann aber sichergestellt werden, dass die Zufallszahlen auf dem Kanal zwischen Anwendungskonnektor und Netzkonnektor weder manipuliert noch mitgelesen werden können.

Es kann sinnvoll sein, den gleichen Zufallszahlengenerator von verschiedenen Teilkomponenten des Konnektors (Netzkonnektor, Anwendungskonnektor) zu nutzen – etwa wenn die gSMC-K über einen geprüften Zufallszahlengenerator verfügt. Dies setzt im Falle einer Mehrkomponenten-Lösung (siehe Abschnitt 7.6.3 Der Konnektor als Mehrkomponenten-Lösung) aber voraus, dass die einzelnen Teilkomponenten sicher miteinander kommunizieren (organisatorischer Schutz wie von A.NK.phys_Schutz gefordert oder technischer Schutz durch sicheren Kanal und vorherige gegenseitige Authentisierung) und geeignete Schnittstellen für die gemeinsame Nutzung von Ressourcen (z. B. Chipkarten) bereitstellen. Der ST-Autor soll dies bei der Formulierung des Security Targets geeignet berücksichtigen.

Wie bei jedem Umgebungsziel gilt auch hier: Wenn der EVG selbst bereits einen geprüften Zufallszahlengenerator hoher Güte und Qualität besitzt, kann dieses Ziel von der Umgebung in den EVG verlagert werden (z. B. O.RNG).

7.6.13. gSMC-K in Verbindung mit einer Software-Lösung für den Netzkonnektor (zu Abschnitt 4.2 Sicherheitsziele für die Umgebung, OE.NK.gSMC-K)

Auch im Fall einer reinen Software-Lösung (z. B. beim Einsatz in einem Krankenhaus) kann auf die gSMC-K nicht verzichtet werden. Die Untrennbarkeit von gSMC-K und Software-Netzkonnektor sowie der Schutz des Kommunikationskanals zwischen gSMC-K und Netzkonnektor gegen Mitlesen und Manipulation muss in diesem Fall organisatorisch sichergestellt werden.

Siehe auch Abschnitt 3.1 („Konnektoridentität“) in der Konnektor-Spezifikation [15]. Dort heißt es u. a.:

„Der Konnektor MUSS das geheime Schlüsselmaterial zur Geräteidentität […] und der Rolle SAK […] über Smartcards des Typs gSMC-K gemäß […] nutzen“

7.6.14. Datenkennzeichnung durch den Anwendungskonnektor, das Clientsystem oder durch weitere Systeme im LAN (zu Abschnitt 4.2 Sicherheitsziele für die Umgebung, OE.NK.AK und OE.NK.CS)

Ob Daten zu schützende Daten der TI *und der Bestandsnetze* im Sinne des § 291 a SGB V sind, wird durch die Clientsysteme bestimmt. Die „Kennzeichnung“ solcher Daten erfolgt daher zunächst im Clientsystem (bzw. durch weitere Systeme oder Komponenten im LAN) durch den Aufruf einer geeigneten Schnittstelle:

den Aufruf eines Fachdienstes nach §291a SGB V [9] an der Clientsystem-Schnittstelle des Anwendungskonnektors (z. B. WriteVO() für „eVerordnung einstellen“) und die Verwendung eines standardisierten Dokumententyps (z. B. eVerordnung, Überprüfung durch XML-Schemaprüfung).

Diese durch das Clientsystem bzw. durch weitere Systeme oder Komponenten im LAN vorgenommene „Kennzeichnung“ muss zunächst einmal korrekt sein (siehe OE.NK.CS). Falls das Clientsystem den Anwendungskonnektor aufgerufen hat, muss der Anwendungskonnektor diese Datenkennzeichnung (mindestens die Klassifizierung als Pflichtanwendung bzw. freiwillige Anwendung der Telematikinfrastruktur) korrekt verarbeiten (siehe OE.NK.AK). Die Common Criteria sprechen in diesem Zusammenhang von Sicherheitsattributen der Benutzerdaten; die technische Realisierung der Datenkennzeichnung ist dem Hersteller jedoch freigestellt. Siehe auch Abschnitt 7.6.9.

In diesem Sinne vom Anwendungskonnektor als zu schützende Daten der TI *und der Bestandsnetze* gekennzeichnete Daten (Daten für Anwendungen gemäß § 291 a SGB V) dürfen vom EVG (Netzkonnektor) ausschließlich gesichert, das heißt über den entsprechenden VPN-Tunnel an die zentrale Telematikinfrastruktur-Plattform weitergeleitet werden (an einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur).

Dabei ist es wichtig, dass der Anwendungskonnektor eine konsequente Trennung von zu schützenden Daten gemäß § 291 a SGB V einerseits und der EVG eine Weiterleitung an einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur andererseits durchsetzen.

7.6.15. Sichere Kanäle

Falls erforderlich, baut der EVG sichere Kanäle zu verteilten dezentralen Komponenten auf. Der ST-Autor soll alle sicheren Kanäle beschreiben, die vom EVG zu verwalten sind.

Neben den sicheren VPN-Tunneln zu VPN-Konzentratoren sind sichere Kanäle zu folgenden dezentralen Komponenten denkbar:

- gSMC-K (falls sich diese nicht im Gehäuse des Konnektors befindet, siehe Anwendungshinweis 49),
- Anwendungskonnektor (im Falle von Mehrkomponenten-Lösungen, siehe auch Abschnitt 7.6.3),
- lokale Administration (falls der Schutz gegen Abhören von Authentisierungsdaten und die Manipulation von administrativen Kommando- und Antwortnachrichten nicht durch die Umgebung geleistet wird),
- zentrale Administration (optional),
- sicheres Software-Update.

Für alle sicheren Kanäle wird – sofern nichts anderes angegeben wird – folgendes gefordert:

- gegenseitige Authentisierung der Enden des sicheren Kanals über Zertifikate,
- Sicherung der Vertraulichkeit der übertragenen Daten (Verschlüsselung) und
- Sicherung der Integrität der übertragenen Daten (Signatur oder MAC-Bildung).

Es ist denkbar, dass ein sicherer Kanal für spezielle Aufgaben weniger Eigenschaften aufweisen muss als hier aufgezählt; dies ist aber im Einzelfall zu begründen. Beispielsweise reicht es für das sichere Software-Update aus, wenn der Konnektor die Authentizität und Integrität der empfangenen Daten überprüft, bevor ein entsprechendes Software-Update aktiviert wird. Die Daten können also über einen ungesicherten Kanal transportiert werden, wenn die Daten selbst integritätsgeschützt und authentisch sind.

Der ST-Autor soll beschreiben, welche Verbindungen durch sichere Kanäle geschützt werden müssen und wie der Schutz vorgenommen wird. Falls erforderlich sind im Zusammenhang mit der Forderung nach sicheren Kanälen im ST ein oder mehrere entsprechende Ziele zu ergänzen.

7.6.16. Emanation Security (zu Abschnitt 6.2.5, FPT_EMS.1/NK)

Die privaten Authentisierungsschlüssel für die VPN-Verbindung werden in der gSMC-K gespeichert und angewendet, so dass keine Berechnung innerhalb des EVG stattfindet. Im

Rahmen der Authentisierung der VPN-Kommunikationspartner wird aber ein Sitzungsschlüssel (session key) abgeleitet, der vom EVG geschützt werden muss, da seine Kompromittierung z. B. einem Angreifer aus dem Internet Zugriff auf das LAN des Leistungserbringers ermöglichen kann.

Falls die Prüfschlüssel zur Verifikation der eigenen Integrität im Rahmen der Selbsttests als öffentliche Schlüssel eines asymmetrischen Kryptoalgorithmus' ausgestaltet sind (z. B.: Verifikation einer Signatur), ist deren Vertraulichkeit nicht zu schützen (der Schutz ihrer Integrität ist in diesem Fall ausreichend). Falls ein symmetrisches Verfahren zum Einsatz kommt (z. B. Prüfung eines MAC), ist die Vertraulichkeit des Schlüssels zu schützen. Gleiches gilt sinngemäß für die Prüfschlüssel zur Verifikation der Integrität und Authentizität von Software-Updates.

Falls Software-Updates in verschlüsselter Form übertragen werden und die Vertraulichkeit der dabei übertragenen Daten im Security Target zu einem Sicherheitsziel für den EVG erhoben wurde, muss der EVG die Vertraulichkeit des Schlüsselmaterials (geheimer symmetrischer oder privater asymmetrischer Schlüssel) schützen, mit dem empfangene Software-Updates entschlüsselt werden. Falls Software-Updates unverschlüsselt übertragen werden bzw. die Vertraulichkeit der bei einem Software-Update übertragenen Daten kein Sicherheitsziel des EVGs darstellt, darf in der Zeile „key material used to decrypt encrypted software updates (if applicable)“ in FPT_EMS.1.1/NK im Security Target die Zuweisung „none“ gewählt werden.

Schließlich muss der EVG die Vertraulichkeit der Geheimnisse, mit denen sich ein Administrator gegenüber dem EVG authentisieren kann, schützen. Der ST-Autor muss entscheiden, ob Angriffe (im Sinne Emanation Security) gegen diese Authentisierung des Administrators betrachtet werden sollen oder nicht. Abhängig von dieser Entscheidung muss der ST-Autor die Zuweisungen in FPT_EMS.1/NK geeignet vornehmen: Falls Angriffe gegen die Authentisierung des Administrators nicht betrachtet werden sollen, darf in der Zeile „key material used for authentication of administrative users“ in FPT_EMS.1.1/NK im Security Target die Zuweisung „none“ gewählt werden.

Die Anforderung FPT_EMS.1.1/NK erzwingt nicht notwendigerweise Penetrationstests, sondern es ist auch denkbar, dass ein Aspekt durch argumentative Nachweise abgedeckt wird. Beispielsweise kann im Rahmen einer Quellcodeanalyse nachgewiesen werden, dass bei einer PIN-Prüfung keine zeitlichen Abhängigkeiten bestehen, die für Angriffe ausgenutzt werden können.

Die Annahme A.NK.phys_Schutz (siehe dort) begrenzt die Angriffsszenarien, die für FPT_EMS.1/NK betrachtet werden müssen.

7.6.17. LAN-seitiger Paketfilter

Der Netzkonnektor (EVG) verfügt grundsätzlich immer über einen LAN-seitigen Paketfilter, der den Netzkonnektor vor potentiellen Angriffen aus dem LAN schützt. Im Fall einer Einbox-Lösung, für den dieses Schutzprofil erstellt wurde, muss dieser LAN-seitige Paketfilter des Netzkonnektors auch den Anwendungskonnektor schützen (vgl. Abbildung 2 in Abschnitt 1.3.2 Einsatzumgebung des Konnektors).

Im Fall einer Mehrkomponenten-Lösung sind Topologien denkbar, bei denen der Netzkonnektor dies nicht leisten kann (vgl. etwa Abbildung 4 in Abschnitt 7.6.3). Daher wird im Fall einer Mehrkomponenten-Lösung gefordert, dass die IT-Einsatzumgebung einen LAN-seitigen Paketfilter für den Anwendungskonnektor bereitstellen soll. Hierzu kann der ST-Autor sinngemäß z. B. folgende Annahme A.PF_LAN und ein dazu korrespondierendes Umgebungsziel OE.PF_LAN einführen:

A.PF_LAN LAN-seitiger Paketfilter

Die IT-Einsatzumgebung stellt dem Mehrkomponenten-Konnektor einen LAN-seitigen Paketfilter bereit, welcher den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt.

7.6.18. Bedrohungen (zu den Abschnitten 3.3.2.1 T.NK.local_EVG_LAN und folgenden sowie zu den Abschnitten 4.3.2.1 T.NK.local_EVG_LAN und folgenden)

Da der EVG (Netzkonnektor) im Fall einer Einbox-Lösung mit seinem LAN-seitigen Paketfilter auch den Anwendungskonnektor schützt, umfasst die Bedrohung T.NK.local_EVG_LAN in Abschnitt 3.3.2.1 im Fall einer Einbox-Lösung auch LAN-seitige Angriffe auf den Anwendungskonnektor. Der ST-Autor soll prüfen, ob in der Formulierung der Bedrohung T.NK.local_EVG_LAN ggf. der Begriff „Konnektor“ statt „Netzkonnektor“ verwendet werden kann bzw. sollte. Im Erklärungsteil in Abschnitt 4.3.2.1 muss der ST-Autor dann in Übereinstimmung mit Abschnitt 3.3.2.1 prüfen, ob die Angriffe sich ausschließlich gegen den EVG (Netzkonnektor) richten oder ob Angriffe gegen den Konnektor allgemein betrachtet und abgewehrt werden. Abhängig davon muss der ST-Autor den Erklärungsteil entsprechend anpassen; im ST sollte der Erklärungsteil keine Fallunterscheidungen mehr enthalten.

Das gleiche gilt sinngemäß auch für weitere Bedrohungen (in den Abschnitten 3.3.2.2 T.NK.remote_EVG_WAN und folgende) sowie für die zugehörigen Erklärungsteile (in den Abschnitten 4.3.2.2 und folgende), die ggf. durch den ST-Autor anzupassen sind:

Zur Bedrohung T.NK.remote_EVG_WAN (Abschnitt 3.3.2.2) ist anzumerken: Der Netzkonnektor schützt nicht nur sich selbst, sondern auch den Anwendungskonnektor. Deshalb werden in dieser Bedrohung ganz allgemein Angriffe auf den „Konnektor“ betrachtet. Gleiches gilt für die Bedrohung T.NK.remote_EVG_LAN (Abschnitt 3.3.2.3).

Zur Bedrohung T.NK.remote_VPN_Data (Abschnitt 3.3.2.4) ist anzumerken: Der Netzkonnektor schützt die Kommunikation zwischen Anwendungskonnektor und zentraler Telematikinfrastruktur-Plattform. Angriffe aus dem WAN richten sich jedoch stets gegen den Netzkonnektor.

In analoger Weise wurden die Begriffe „Netzkonnektor“ und „Konnektor“ in der Formulierung der Bedrohungen T.NK.local_admin_LAN und T.NK.remote_admin_WAN (Abschnitte 3.3.2.5 und 3.3.2.6) verwendet und sind ggf. vom ST-Autor geeignet anzupassen.

Zur Bedrohung T.NK.counterfeit (Abschnitt 3.3.2.7) ist anzumerken: Im Fall einer Einbox-Lösung ist die Tatsache, dass ein Angreifer gefälschte Netzkonnektoren in Umlauf bringt, gleichbedeutend mit dem In-Umlauf-Bringen gefälschter Konnektoren.

7.7. Literaturverzeichnis

7.7.1. 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

7.7.2. Gesetze und Verordnungen

[9] Fünftes Buch Sozialgesetzbuch (SGB V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477), zuletzt geändert durch Artikel 6 des Gesetzes vom 28. Mai 2008 (BGBl. I S. 874)

7.7.3. Schutzprofile (Protection Profiles) und Technische Richtlinien

[10] Common Criteria Protection Profile: Card Operating System (PP COS), BSI-CC-PP-0082-V2-2014, Version 1.9 vom 18.11.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Common Criteria Protection, Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Version 1.5.4 vom17.03.2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Technische Richtlinie TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Bundesamt für Sicherheit in der Informationstechnik, Version 2019-01

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

[14] 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

7.7.4. Spezifikationen

[15] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec_Kon], gematik GmbH, PTV3: Version 5.4.0, 26.10.2018, zuzüglich der Errata 1 bis 6 für den PTV3 Konnektor, PTV4: Version 5.9.0, 02.03.2020

[16] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik GmbH, Version 1.17.0, 02.03.2020

[17] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik GmbH, Version 2.16.0, 02.03.2020

[18] Einführung der Gesundheitskarte: Spezifikation des Card Operating System (COS) Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik GmbH

[19] Einführung der Gesundheitskarte: Spezifikation der gSMC-K / Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.12.0, 15.05.2019, gematik GmbH

7.7.5. Standards

[20] 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

[21] 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

[22] 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

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

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

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

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

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

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

[29] 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

[30] T. Kivinen, B. Swander, A. Huttunen, V. Volpe: Negotiation of NAT-Traversal in the IKE, January 2005, RFC 3947 (NAT-Traversal in IKE) http://www.ietf.org/rfc/rfc3947.txt

[31] 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

[32] 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

[33] 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

[34] 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

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

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

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

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

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

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

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

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

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

[44] 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

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