Sicherheitsvorgaben

für den

Medical Access Port_1BK_1.0.0 Netzkonnektor

Bauform Einboxkonnektor 1.5

BSI-DSZ-CC-0928-V2

Dokumentversion 2.14

T-Systems International GmbH
Hahnstraße 43d
D-60258 Frankfurt am Main

Zusammenfassung

Das vorliegende Dokument enthält die Sicherheitsvorgaben für die Evaluierung des Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5. Der Text stützt sich wesentlich auf das Schutzprofil des Netzkonnektors [47], wurde jedoch zur Berücksichtigung des Besonderheiten des Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 angepasst.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Die folgenden Abschnitte enthalten allgemeine Informationen über den Evaluierungsgegenstand (EVG), dieses Dokument und weitere Angaben.

1.1 Referenzen

Titel des Dokumentes:	Sicherheitsvorgaben für den Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Dokumentversion 2.14 vom 6.9.2019
Dokumentversion:	2.14
Datum des Dokumentes:	6.9.2019
Status des Dokumentes:	Finale Version
EVG:	Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5
Version des EVGs (Produktversion):	Version 1.5.3 Build 43
Common Criteria Referenz:	CC, Version 3.1, Revision 5, April 2017
Vertrauenswürdigkeit:	EAL3+, d. i. EAL3 mit Zusatz von AVA_VAN.5 und ALC_FLR.2 unter Berücksichtigung der Abhängigkeiten
Entwickler:	T-Systems International GmbH, Hahnstraße 43d, D-60528, Frankfurt am Main
Zertifizierungs-ID:	BSI-DSZ-CC-0928-V2

1.2 EVG-Überblick

Der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5[1] ist Teil der Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens[2] und den Client-Systemen des Gesundheitswesens. Die elektronische Gesundheitskarte (eGK), der Heilberufsausweis (HBA), die Institutskarte (SMC-B, Security Module Card Typ B), der Hardware-Sicherheitsmodul HSM-B, die Kartenterminals und die Konnektoren bilden die dezentralen Komponenten der Telematikinfrastruktur. Zu den Client-Systemen gehören die Praxisverwaltungssysteme der Ärzte (PVS), die Krankenhausinformationssysteme (KIS) und die Apothekenverwaltungssysteme (AVS). Der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 stellt auch eine gesicherte Verbindung zu einem Sicheren Internet Service (SIS) bereit.

Der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 umfasst die folgenden (Sicherheits-)funktionalitäten:

- Einen VPN[3]-Client zur IPsec[4]-gesicherten Kommunikation mit der Telematikinfrastruktur (TI) und dem sicheren Internet-Service
- Eine Firewall zur Sicherung der Kommunikationskanäle Local Area Network (LAN) und Wide Area Network (WAN)
- Zeitsynchronisation mit einem Zeitdienst in der Telematik-Infrastruktur (TI) und Bereitstellung eines Stratum 3 Zeitsignals auf der Seite des Leistungserbringers
- Domain Name System (DNS)-Funktionalität zur Auflösung gegebener Full Qualified Domain Name (FQDN)-Anfragen in IP-Adressen[5]
- Automatische (Adress-)konfiguration der Netzwerkschnittstellen[6]
- Authentisierung des Administrators des Konnektors aus dem Netz des Leistungserbringers und Bereitstellung einer Managementschnittstelle

[1] Die Verwendung des Begriffs Medical Access Port_1BK_1.0.0 Netzkonnektor ist synonym zu Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5.

[2] 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.

[3] Virtual Private Network (VPN)

[4] Internet Protocol Security (IPSEC)

[5] Der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 beinhaltet sowohl einen DNS-Stub Resolver, der auf der LAN-Seite ansprechbar ist als auch einen DNSSEC-Client, der im WAN DNSSEC-Anfragen stellt. Der Netzkonnektor unterstützt ausschließlich IPv4-Adressen.

[6] Der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 beinhaltet einen Dynamic Host Configuration Protocol (DHCP)-Client, der die automatische Adresszuweisung vornimmt. Neben der Adresse werden weitere Parameter wie das Standard-Gateway konfiguriert. Ebenso ist die Zuweisung einer statischen IP-Adresse möglich.

- Vertrauenswürdige Kommunikationskanäle auf Basis von TLSv1.2 in das Netz der Leistungserbringer und im WAN zum sicheren Internet Service[7]
- Updates der Firmware. Die umfasst sowohl das eingesetzte Unified Extensible Firmware Interface (UEFI), das Betriebssystems, Netz- und Anwendungskonnektorspezifische Dienste sowie Fachmodule

1.3 EVG-Beschreibung

Der Evaluationsgegenstand (EVG) ist ein Softwareprodukt, das Anforderungen der Konnekorspezifikation (insbesondere des Netzkonnektors) umsetzt und Sicherheitsfunktionalität konform zum Schutzprofil des Netzkonnektors [47] anbietet. Der Netzkonnektor ist Teil des Gesamtproduktes *MAP - Medical Access Port - Einboxkonnektor 1.5* und wird gemeinsam mit einer zugehörigen Hardware ausgeliefert.

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[8] bereit. Das Gesamtprodukt setzt sich demnach aus Netz- und Anwendungskonnektor, gSMC-K und Fachmodulen zusammen. Der Netzkonnektor stellt Paketfilter- und VPN-Funktionalität für die Kommunikation mit der zentralen Telematikinfrastruktur-Plattform und einem sicheren Internet-Service bereit. Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssystem und dem Objektsystem für die gSMC-K. Sie speichert Schlüsselmaterial für den Netz- und Anwendungskonnektor und stellt kryptographische Sicherheitsfunktionen bereit. Die Sicherheitsfunktionalität des Anwendungskonnektors umfasst die Signaturanwendung, die Verschlüsselung und Entschlüsselung von Dokumenten, den Kartenterminaldienst, den Chipkartendienst, die gesicherte Kommunikation zwischen dem Konnektor und dem Client-System sowie zwischen Fachmodulen und Fachdiensten bzw. Intermediären. Die Abbildung 1.1 zeigt eine schematische Darstellung des Konnektors.

Der EVG Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 realisiert **nicht** den gesamten Konnektor, sondern nur den in Abbildung 1.1 mit NK bezeichneten Teil. Der EVG umfasst die Software des Netzkonnektors und die zugehörige Betriebsdokumentation. Die verwendete Hardware ist eine in einem weißen Kunststoffgehäuse befindliche Intel-Architektur, welche die zur Nutzung des EVGs erforderlichen Hardware-Schnittstellen[9]anbietet. Bestandteil dieser Hardwareumgebung ist die gSMC-K, die vom EVG für den Umgang mit kryptografischen Schlüsseln und Zufallszahlen genutzt wird.

[7]Der Geltungsbereich dieser Betrachtung bezieht sich dabei ausschließlich auf die Kommunikationskanäle bei der Administration.

[8]Fachmodul (FM)

[9]Ethernet-Schnittstellen, LEDs und 7-Segment Anzeigen, Slot zur Aufnahme der gSMC-K, RTC-Baustein

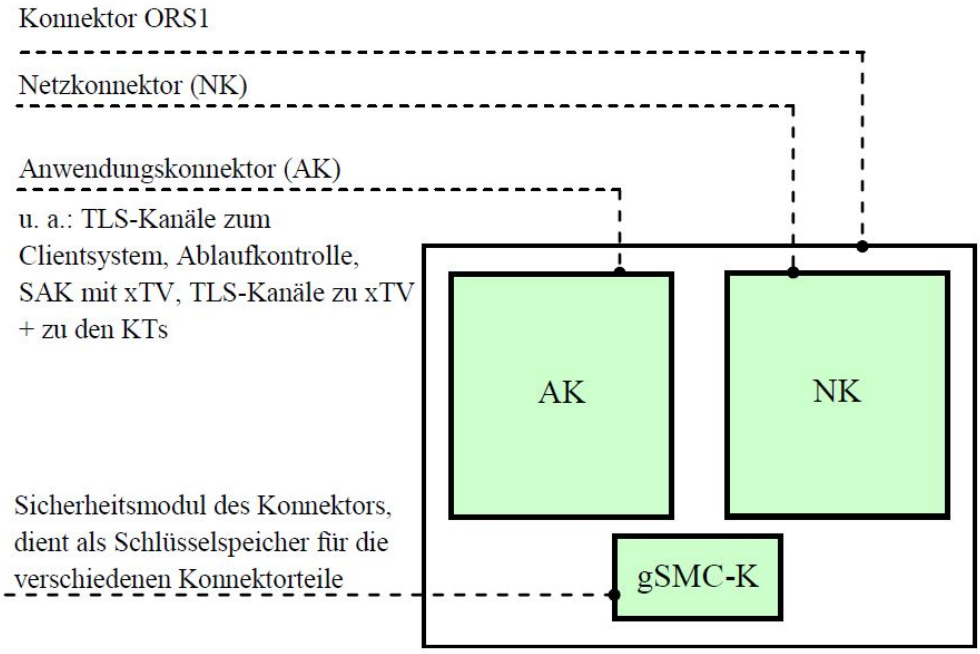


Abbildung 1.1: Schematische Darstellung des Konnektors

Der EVG besteht aus mehreren Artefakten, die in Ihrer Gesamtheit die Bezeichnung Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 tragen. Die Einzelartefakte und deren Versionsbezeichnungen werden in Tabelle 1.1 aufgeführt.

Tabelle 1.1: Artefakte des Netzkonnektors

Artefakt	**Erläuterung**
UEFI Version S1.40.1.1	Das UEFI zur Initialisierung der Hardware und Start des Betriebssystems
Linux-Betriebssystem Version 3.16 Patchstand 57[10]	Das verwendete Betriebssystem, welches zugleich Teil des EVGs ist.
Netzkonnektorsoftware Version 1.5.3, Build 43, Ausprägung Einboxkonnektor[11]	Die Software des Netzkonnektors. Diese beinhaltet unter anderem den VPN-Client und die Managementfunktionalität.
Produkthandbuch T-Systems Konnektor, Version 1.30 [58]	Das Anwenderhandbuch zum Netzkonnektor. Der SHA-256 Hashwert des Benutzerhandbuchs wird im Zertifizierungsbericht veröffentlicht.

Fortsetzung auf der nächsten Seite

[10] Dies Artefakt ist Bestandteil der Netzkonnektorsoftware und über dessen Versionsnummer eindeutig zuordenbar.

[11] In der Management-Oberfläche wird der Artefakt als „Telekom-Konnektor EBK (TKONEBK) in der Produktversion 1.5.3 - Build: 43 - Revision: 0fcda6efe2“ angezeigt.

Artefakt	**Erläuterung**
Schnittstellenspezifikation T-Systems Netzkonnektor[59]	Handbuch mit Dokumentation der programmierbaren Schnittstelle. Nur auf Anfrage und nur unter Vorbehalt erhältlich. Der SHA-256 Hashwert des Handbuchs zur Programmierschnittstelle wird im Zertifizierungsbericht veröffentlicht.

Die Versionen des UEFI, des Betriebssystems und der Netzkonnektorsoftware wird in der Managementoberfläche des EVGs angezeigt. Während des Starts führt der EVG einen Selbsttest zur Verifikation seiner Integrität durch. Der Nutzer kann diesen Selbsttest durch Auslösen eines Neustarts initiieren.

Die Inbetriebnahme des EVGs muss durch einen Administrator erfolgen. Der EVG wird mit einem aktivierten Standardzugang ausgeliefert. Im Zuge der ersten Anmeldung eines Administrators muss dieser vorgegebene Standardkennwort ändern. Die Unversehrtheit der empfangenen Auslieferung ist für den Administrator an Hand der folgenden Eigenschaften erkennbar:

- Das angebrachte Siegel an der ausgelieferten Hardware ist unverändert und weist keine Beschädigungen auf
- Der Standardaccount zum Zugriff auf die Managementoberfläche des Netzkonnektors ist unverändert
- In der Managementoberfläche wird die korrekte Revision der Software angezeigt

Ein weiteres Indiz für die unversehrte Auslieferung ist, dass der EVG auf der Hardwareplattform überhaupt zur Ausführung gebracht werden kann. Während des Startvorgangs führt der EVG einen Integritäts- und Authentizitätstest durch. Schlägt dieser fehl, wird der Startvorgang abgebrochen und es wird mithilfe der 7-Segment Anzeige ein Fehlercode dargestellt.

1.3.1 EVG-Typ

Der EVG ist ein Produkt. Es umfasst die in 1.2 aufgeführten Sicherheitsfunktionalitäten.

Der Begriffsbildung des Schutzprofils [47] folgend, stellt der *Konnektor* einen neuen Produkttyp dar. Da der Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 jedoch lediglich einen Teil der Funktionalität eines *Konnektors* bereitstellt[12], kann als EVG-Typ hier nur *Teil eines Konnektors* angegeben werden.

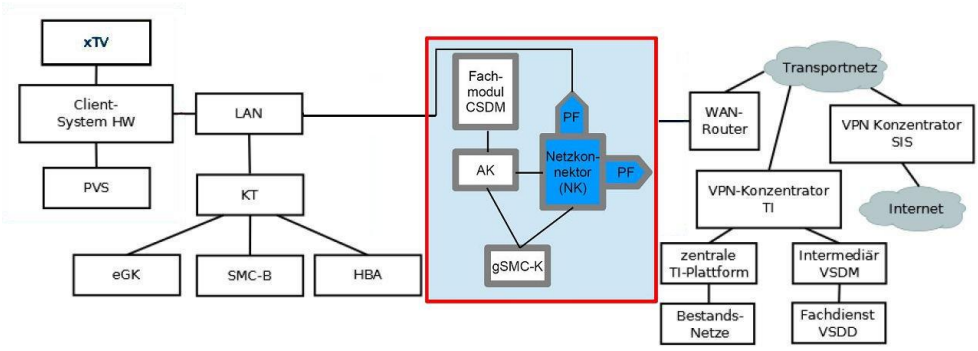


Abbildung 1.2: Darstellung der Einsatzumgebung

1.3.2 Einsatzumgebung des Netzkonnektors

Die Einsatzumgebung des Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 ist in der Abbildung 1.2 dargestellt. Insbesondere wird der Netzkonnektor immer mit weiteren Konnektorteilen (AK, gSMC-K) gemeinsam betrieben. Netzkonnektor und Anwendungskonnektorwerden in einem Gehäuse verbaut; Netzkonnektor und Anwendungskonnektor greifen auf dieselbe gSMC-K zu.

Die in Abbildung 1.2 links vom Transportnetz dargestellten Komponenten befinden sich im lokalen Netz (LAN) des Leistungserbringers und werden als dezentrale Komponenten bezeichnet. Der oder die VPN-Konzentratoren und die übrigen rechts und unterhalb vom Transportnetz dargestellten Dienste werden als zentrale Dienste oder zentrale Telematikinfrastruktur-Plattform bezeichnet.

Alle Teilkomponenten des Konnektors sind durch dicke graue 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, der WAN-seitige Paketfilter ist also Teil des EVG. Die rote Umrandung umschließt die Komponenten, die in einem gemeinsamen Gehäuse untergebracht sind.

Neben den dargestellten physikalischen Verbindungen gibt es logische Kanäle, die über die physikalischen Verbindungen etabliert werden und üblicherweise zusätzlich geschützt werden (sichere Kanäle). Diese Verbindungen sind in der Abbildung 1.2 aus Gründen der Übersichtlichkeit nicht dargestellt.

Es ist jedoch deutlich, dass Anwendungskonnektor und Netzkonnektor die gleiche gSMC-K nutzen.

In Abbildung 1.2 werden folgende Abkürzungen benutzt:

Tabelle 1.2: Bildlegende Abbildung 1.2

Kürzel	**Erläuterung**
NK	Netzkonnektor
AK	Anwendungskonnektor
xTV	Extended Trusted Viewer, sichere Anzeigekomponente der SAK

[12]Konkret den Netzkonnektor

KT (= eHealth KT)	Kartenterminal im Gesundheitswesen; aus Gründen der Übersichtlichkeit ist 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.
Client-System-HW	Hardware des Client-Systems. Auf dieser Plattform läuft die Software des Leistungserbringers (z. B. Praxisverwaltungssystem, Apothekenverwaltungssystem, Krankenhaus-Informationssystem). Im Allgemeinen wird dort auch die Darstellungskomponente des Extended Trusted Viewers ablaufen. Vereinfachend wird diese Darstellungskomponente kurz als xTV bezeichnet.
PVS	Praxis-Verwaltungssystem. Dieser Ausdruck steht stellvertretend auch für Apotheken-Verwaltungssysteme (AVS) oder Krankenhaus-Informationssysteme (KIS). Er bezeichnet den Softwareanteil auf dem Client-System. Das Betriebssystem des Client-Systems ist nicht dargestellt.
eGK	elektronische Gesundheitskarte
HBA	Heilberufsausweis
SMC-B	Security Module Card, Typ 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

Der EVG ist für den Einsatz in normalen Arbeitsumgebungen, z. B. in Arztpraxen konzipiert und verfügt daher über die nachfolgend aufgeführten, zusätzlichen physischen Schutzmechanismen.

- Das Gehäuse ist so aufgebaut, dass eine Kontaktierung der Platine ohne Entfernung des Gehäuses nicht möglich ist. Ein von außen auf dem Gehäuse angebrachtes Siegel verhindert eine unerkannte Öffnung des Gehäuses.
- Zur optischen Signalisierung von (Fehler-)zuständen dienen zwei 7-Segment Anzeigen und drei LEDs. Ihre Bedeutung und die ggf. vom Betreiber vorzunehmenden Handlungen werden im zum Lieferumfang gehörenden Handbuch beschrieben.
- Die gSMC-K befindet sich im Gehäuse und ist mit der Hardware des EVGs dauerhaft verbunden.

1.3.3 Schnittstellen des Netzkonnektors

1.3.3.1 Physische Schnittstellen des EVGes

Der Netzkonnektor verfügt über die im Folgenden aufgelisteten physischen Schnittstellen[13].

Tabelle 1.3: Physische Schnittstellen des EVGs

Kürzel	**Erläuterung**
PS1	Physische Schnittstelle zum Anwendungskonnektor.
PS2	Schnittstelle zum LAN. Über diese Schnittstelle können Client-Systeme oder andere Systeme im LAN mit dem Konnektor kommunizieren.
PS3	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.[14]

Fortsetzung auf der nächsten Seite

[13] In Tabelle 1.3 mit PS abgekürzt.

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

Kürzel	Erläuterung
PS4	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 Public-Key-Infrastructure (PKI) 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.
PS5	Die Schnittstelle zum RTC-Baustein der Hardware. Der EVG synchronisiert seine Systemzeit mit der Zeitangabe des RTC-Bausteins. Darüber hinaus synchronisiert der EVG die Referenzzeit des RTC-Bausteins mit dem Zeitsignal des Stratum-2 Zeitservers der TI.
PS6	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.

1.3.3.2 Logische Schnittstellen des EVG

Der EVG besitzt folgende logische Schnittstellen:

Tabelle 1.4: Logische Schnittstellen des EVGs

Kürzel	Erläuterung
LS1	Schnittstelle zum Anwendungskonnektor (via PS1)
LS2	Schnittstelle zu den Client-Systemen im LAN (via PS2)
LS3	Schnittstelle zur entfernten Telematikinfrastruktur via VPN und WAN (PS3)
LS4	Schnittstelle zum SIS via VPN und WAN (PS3)
LS5	Schnittstelle zum ungesicherten Transportnetz (WAN, via PS3)
LS6	Schnittstelle zu Managementfunktionen des Netzkonnektors (via PS1)
LS7	Schnittstelle zu einem Sicherheitsmodul für den Netzkonnektor (gSMC-K) (via PS4)
LS8	Schnittstelle zum RTC-Baustein der Hardware-Umgebung (via PS5)

1.3.4 Betriebsmodi des EVGs

Die Funktionsweise des EVGs als (VPN-)Konnektor zwischen dem Netz des Leistungserbringers und der TI sowie dem Internet unter Nutzung des Sicherer Internet-Service (SIS) ist von den Betriebsparametern *Leistungsumfang*, *Anbindungsmodus*, *Internet-Modus* abhängig. Diese werden in den nachfolgenden Abschnitten erklärt. Es ist zu beachten, dass die gewählten Betriebsparameter ebenfalls Einfluss auf das Verhalten des Anwendungskonnektors und der Fachmodule haben können.

1.3.4.1 Leistungsumfang

Der Betriebsparameter *Leistungsumfang* entscheidet, ob der EVG über das Transportnetz eine VPN-Verbindung zur TI und zum SIS aufbaut. Der Betriebsparameter *Leistungsumfang* ist als Menge mehrerer Einzelparameter zu verstehen.

$$\begin{aligned} Leistungsumfang = \\ \{&MGM\_LU\_ONLINE, \\ &MGM\_STANDALONE\_KON, \\ &MGM\_LOGICAL\_SEPARATION\} \end{aligned}$$

Tabelle 1.5: Einzelparameter des Betriebsparameters Leistungsumfang

Einzelparameter	**Erläuterungen**
MGM_LU_ONLINE	Dieser Parameter entscheidet, ob der EVG überhaupt eine Online-Kommunikation erlaubt. Ist dieser auf *Disabled* gestellt, so kommuniziert der EVG ausschließlich mit dem Netz des Leistungserbringers und angeschlossenem Intranet[15].
MGM_STANDALONE_KON	Das Setzen von MGM_STANDALONE_KON auf *Enabled* dient dem Konnektor als Anzeige, dass dieser ohne angeschlossenes Client-System (Primärsystem) betrieben wird. Diese Information **kann** seitens der Fachmodule verwendet werden, damit diese sich im Standalone-Fall anders als im Normalfall verhalten. Die Funktionalität des EVGs hinsichtlich seiner erbrachten Netzdienste wird von diesem Parameter nicht beeinflusst.

Fortsetzung auf der nächsten Seite

Einzelparameter	**Erläuterungen**
MGM_LOGICAL_SEPARATION	Wird dieser Parameter auf *Enabled* gesetzt, so unterbindet der EVG die Kommunikation zwischen den Netzen des Leistungserbringers und der TI. Zudem erlaubt der EVG **keine** Kommunikation aus den Netzen des Leistungserbringers mit dem Internet unter Verwendung des SIS. Unabhängig davon ist es jedoch Fachmodulen gestattet, mit der TI zu kommunizieren.

1.3.4.2 Anbindungsmodus

Der Anbindungsmodus wird zur Integration des EVGs in eine bestehende Netzinfrastruktur genutzt. So kann der EVG zwischen dem lokalen Netz und dem Internet Access Gateway (IAG) aufgestellt werden, so dass sämtlicher ans Weitverkehrsnetz gerichtete Datenverkehr über den EVG vermittelt wird. Dieser Modus hat die Bezeichnung *InReihe*. Der EVG kann in diesem Szenario als Default-Gateway für diejenigen Geräte im Netz des Leistungserbringers agieren, die mit dem Weitverkehrnetz kommunizieren wollen. Eine Alternative ist die Aufstellung des EVGs als Gerät innerhalb einer bestehenden Netzinfrastruktur. In diesem Falle verhält sich der EVG wie ein weiteres in dem Netz befindliches Gerät und bietet seine Dienste innerhalb des Netzsegments des Leistungserbringers an. Dieser Modus wird als *Parallel* bezeichnet.

Der Betriebsparameter zum Anbindungsmodus hat die Bezeichnung ANLW_ANBINDUNGS_MODUS. Für diesen Betriebsparameter sind nur die Belegungen *InReihe* und *Parallel* zulässig.

Tabelle 1.6: Anbindungsmodi des EVGs

Anbindungsmodi	**Beschreibung**
InReihe	Diese Konfiguration ist geeignet für Szenarien, in denen der Konnektor zwischen das lokale Netz und das Internet Access Gateway (IAG) (z. B. Router mit DSL-/Kabelmodem) geschaltet wird.
Parallel	Diese Konfiguration ist geeignet für Szenarien, in denen der Konnektor als weiteres Gerät in die bestehende Netzwerkinfrastruktur integriert wird.

[15] Die Konnektorspezifikation [16] unterscheidet zwischen dem Netz des Leistungserbringers und zwischen Netzsegmenten, die über Routen durch das Netz des Leistungserbringers erreichbar sind. Dazu definiert [16] die Variable ANLW_LEKTR_INTRANET_ROUTES und formuliert die Anforderung *TIP1-A_4724 LAN-Adapter*, wonach der EVG ausgehend vom LAN-Adapter nur mit Adressen im Netz des Leistungserbringers und Adressen in einem der in ANLW_LEKTR_INTRANET_ROUTES verwalteten Segmente kommunizieren darf.

1.3.4.3 Internet-Modus

Der EVG kann Datenverkehr aus dem Netz des Leistungserbringers zum Internet auf verschiedene Arten und Weisen behandeln.

- Der Datenverkehr wird in einen bestehenden VPN-Tunnel zum *SIS* weitergeleitet. In diesem Falle ist der Betriebsparameter ANLW_INTERNET_MODUS auf den Wert SIS eingestellt.
- Der EVG verhält sich wie ein RFC 1812-konformer Router und beantwortet Routing-Anfragen ins Internet mit einer Internet Control Message Protocol (ICMP)-Redirect Nachricht, so dass Clients im Netz des Leistungserbringers die Route über das konfigurierte Internet Access Gateway (IAG) zur Kommunikation mit dem Internet verwenden. In diesem Falle ist der Betriebsparameter ANLW_INTERNET_MODUS auf den Wert IAG eingestellt.
- Über den EVG ist aus dem Netz des Leistungserbringers keine Kommunikation mit dem Internet möglich. In diesem Falle ist der Betriebsparameter ANLW_INTERNET_MODUS auf KEINER eingestellt.

Grundsätzlich routet der Konnektor im Modus ANLW_INTERNET_MODUS=SIS alle für das Internet bestimmten Pakete von Clients, die ihn als Default Gateway verwenden, in den VPN-Tunnel zum SIS, während er im Modus ANLW_INTERNET_MODUS=Keiner diese Pakete verwirft.

Im Unterschied zu (ANLW_ANBINDUNGS_MODUS = InReihe) ist die Nutzung des SIS bei (ANLW_ANBINDUNGS_MODUS = Parallel) optional. Alternativ können auch die Clients, die den Konnektor als Default Gateway verwenden, per Redirect direkt ins Internet verwiesen werden (ANLW_INTERNET_MODUS=IAG).

Tabelle 1.7: Kommunikation Internet und Anbindungsmodus

	Internet Modus		
Anbindung	**Keiner**	**SIS**	**IAG**
InReihe	DROP[16]	FORWARD[17]	N/A[18]
Parallel	DROP	FORWARD	ICMP REDIRECT

Erläuterung: Der EVG erlaubt im Anbindungsmodus *InReihe* die Verwendung des Internetanbindungsmodus *IAG* nicht.

[16] Der Datenverkehr wird verworfen

[17] Der Datenverkehr wird aus dem Netz des Leistungserbringers in den VPN-Tunnel zum SIS weitergeleitet.

[18] Nicht unterstützt / Nicht konfigurierbar

1.3.5 Vom EVG erbrachte Dienste

Der EVG erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [16] definierten Schnittstellen weitgehend automatisch. Der EVG ermöglicht ein Management (Administration) nach Autorisierung des Administrators. Die Authentisierung des Administrators erfolgt durch den Netzkonnektor und kann vom Anwendungskonnektor nachgenutzt werden.

1.3.5.1 Sicherheitsdienste

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. 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 Internet-Providers sowie eine Paketfilterung (IP-Firewall) zur Verfügung. 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.

VPN-Client und Betrieb IPSEC-gesicherter Verbindungen: Der EVG handelt mit Hilfe eines VPN-Clients die kryptografischen Parameter für einen sicheren Kanal (VPN) zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) als auch zum sicheren Internet-Service (SIS) aus und stellt diesen von ihm betriebenen IPSEC-gesicherten Kanal im Tunnel-Modus zwecks Nutzung von Diensten bereit. Der sichere Kanal zur TI wird zur Kommunikation zwischen Anwendungskonnektor, Fachmodulen des Anwendungskonnektors und Fachdiensten, Netzkonnektor und zentralen Diensten sowie zwischen Client-Systemen und Bestandsnetzen genutzt. Der sichere Kanal zum SIS dient der Verbindung der lokalen Netzwerke der Leistungserbringer mit dem Internet. Der EVG setzt **keine** Maßnahmen zur Verschleierung des IPSEC-gesicherten Datenverkehrs mittels Traffic Flow Confidentiality (TFC) um.

1. Der EVG erzwingt die Authentisierung des Kommunikationspartners (VPN-Konzentrator und SIS) und ermöglicht eine Authentisierung gegenüber diesen Partnern; diese erfolgt auf der Basis des IKEv2-Protokolls (vgl. [48]) und mit Hilfe von Zertifikaten nach dem Standard X.509v3 (vgl. [49]). Siehe auch *Sicherheitsdienst Gültigkeitsprüfung von Zertifikaten.*

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

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

Der Netzkonnektor erzwingt die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen und verbietet ungeschützten Zugriff auf das Transportnetz.

Der Betrieb des Tunnels zum SIS setzt eine entsprechende Konfiguration des EVGs voraus und ist demnach optional. Es gelten die im Abschnitt 1.3.4 dargestellten Abhängigkeiten.

Dynamischer Paketfilter: Der EVG bindet die Client-Systeme sicher an die Telematikinfrastruktur an. Dazu verfügt der EVG über einen dynamischen Paketfilters, welcher die im Security Target angegebenen Regeln umsetzt. Der EVG schützt das lokale Netz des Leistungserbringers und sich selbst vor Angriffen aus dem Transportnetz. Zusätzlich schützt sich der EVG vor Angriffen aus dem lokalen Netz des Leistungserbringers. Es 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 TI werden vom Netzkonnektor nicht ausgewertet. In Abhängigkeit von seiner Konfiguration unterbindet der EVG sämtliche weitere Kommunikation in das Transportnetz mit Ausnahme der für den Aufbau[19]und den Betrieb der VPN-Verbindungen erforderlichen Kommunikation.

1.3.5.2 Netzbasierte Dienste

Zeitdienst: Der Netzkonnektor stellt einen NTP-Server der Stratum-3-Ebene für Konsumenten im Netz des Leistungserbringers 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 genutzt, um die Audit-Daten des Sicherheits-Logs mit einem Zeitstempel zu versehen.

DHCP-Dienst: Der EVG stellt an der LAN-Schnittstelle (PS2) die Funktion eines DHCP-Servers gemäß RFC 2131 [43] und RFC 2132 [44] zur Verfügung.

DNS-Dienst: Der EVG stellt an der LAN-Schnittstelle (PS2) und an der Schnittstelle zum AK (PS1) die Funktion eines DNS-Servers zur Verfügung. Der DNS-Server unterstützt DNSSEC-Erweiterungen gemäß RFC 4035 [45]. Die für DNSSEC verwendeten Vertrauensanker werden regelmäßig aktualisiert.

Gültigkeitsprüfung von Zertifikaten: Der EVG prüft die Gültigkeit der Zertifikate des Kommunikationspartners, die für den Aufbau eines VPN-Kanals verwendet werden. Zu diesem Zweck wird eine TSL verteilt, welche Zertifikate von Diensteanbietern enthält, die Gerätezertifikate ausstellen können. Der EVG kann anhand der TSL die Gültigkeit der Gerätezertifikate seiner Kommunikationspartner entlang der Kette prüfen. Ferner wird eine CRL (Certificate Revocation List) bereitgestellt, die der EVG während des Aufbaus des IPsec-Tunnels auswertet. Außerdem überprüft der EVG implizit, dass die verwendeten Algorithmen noch gültig sind.

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

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

1.3.5.3 Übergeordnete Dienste

Firmware-Updates: Der EVG kann Firmware-Updates aus einer (sicheren) Quelle herunterladen und nach einer Prüfung als Firmware installieren. Zusätzlich bietet der EVG die Möglichkeit der Initiierung eines Firmware-Updates über die Managementoberfläche an. Er setzt das von der gematik definierte Firmware-Gruppenkonzept gemäß [57], Abschnitt 2.5 um.

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 Sitzungsschlüssel[20]für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben.

Selbsttests: Der EVG bietet seinen Benutzern eine Möglichkeit, die Integrität des EVGs zu überprüfen, und macht dadurch sicherheitstechnische Veränderungen am EVG für den Anwender erkennbar.

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

Administration: Der EVG bietet eine Managementschnittstelle an. Der EVG erzwingt eine sichere Authentisierung des Administrators vor administrativen Aktivitäten. Dazu nutzt er die Authentisierung des Administrators am Anwendungskonnektor nach. Als technische Mittel zur Identifikation und Authentisierung werden Nutzername und Passwort verwendet.

Eine detailliertere Beschreibung der Sicherheitsdienste findet sich im Kapitel 7.

[20]Session Keys

Kapitel 2

Konformitätserklärungen

2.1 Konformität zu den Common Criteria

Diese Sicherheitsvorgaben wurden gemäß Common Criteria Version 3.1 Revision 5 erstellt.

Es wurde eine funktionale Sicherheitsanforderung (FPT_EMS.1/NK, siehe Kapitel 5) definiert, die nicht in CC Teil 2 [2] enthalten ist. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [3] entnommen.

Daher sind diese Sicherheitsvorgaben :

- CC Teil 2 [2] **erweitert** (extended) und
- CC Teil 3 [3] **konform** (conformant).

2.2 Konformität zum Schutzprofil

Diese Sicherheitsvorgaben sind konform zum Schutzprofil BSI-CC-PP-0047 [47].

Im Schutzprofil wird strikte Konformität gefordert. Daher behaupten diese Sicherheitsvorgaben **strikte Konformität**.

2.3 Konformität zu Vertrauenswürdigkeitspaketen

Diese Sicherheitsvorgaben fordern die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponente AVA_VAN.5. Die Abhängigkeiten dieser Erweiterung werden berücksichtigt, indem die Vertrauenswürdigkeitsstufe EAL3 erweitert wird um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 und (wegen der weiteren Abhängigkeit) ALC_TAT.1. Zusätzlich wird EAL3 um ALC_FLR.2 ergänzt.

Daher sind diese Sicherheitsvorgaben **EAL3 mit Zusatz** (augmented).

Kapitel 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.

Die symbolischen Bezeichner sind mit einem zusätzlichen Kürzel „NK“ versehen (z.B. eine Annahme „Sichere Telematikinfrastruktur“ wird mit A.NK.sichere_TI bezeichnet). Damit wird klargestellt, dass diese sich auf den Netzkonnektor beziehen.

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 (vgl. 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 TI bzw. in die Bestandsnetze übergehen, und umgekehrt. Diese Daten sind User Data im Sinne der Common Criteria. Sie umfassen bei den Pflichtanwendungen nach §291a SGB V [9] mindestens die Versichertenstammdaten[1]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:

[1]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.

- **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.

3.1.1 Primäre Werte

Die primären Werte sind in der folgenden Tabelle 3.1 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder 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-Plattformwerden 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.remote_VPN_Data, A.NK.AK
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.remote_VPN_Data, A.NK.AK

Fortsetzung auf der nächsten Seite

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder erforderliche Annahmen
in der zentralen Telematikinfrastruktur-Plattform oder auf Chipkarten 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. Das gleiche gilt sinngemäß für *zu schützende Daten der TI und der Bestandsnetze*, die auf Chipkarten abgelegt werden. ⇒ T.NK.remote_VPN_Data, A.NK.sichere_TI
Client-System, Anwendungskonnektor	Integrität	Manipulierte Client-Systeme oder Anwendungskonnektoren können dazu führen, dass *zu schützende Daten der TI und der Bestandsnetze* abfließen oder unautorisiert verändert werden. Im normalen Betrieb wird davon ausgegangen, dass *zu schützende Daten der TI und der Bestandsnetze* das Client-System 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 Client-System 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

Fortsetzung auf der nächsten Seite

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder erforderliche Annahmen
Systeme der zentralen Telematikinfrastruktur-Plattform	Verfügbarkeit	Der Anwendungskonnektor kann Syntaxprüfungen und Plausibilisierungen von Anfragen an die zentrale Telematikinfrastruktur-Plattform durchführen und auf diese Weise dazu beitragen, dass weniger nicht wohlgeformte Anfragen an die zentrale Telematikinfrastruktur-Plattform gerichtet werden. Bei diesen Aspekten handelt es sich aber um Bedrohungen der zentralen Telematikinfrastruktur-Plattform und nicht um Bedrohungen des EVG. Außerdem kann der Konnektor nicht für die Verfügbarkeit von Diensten garantieren; daher wird Verfügbarkeit nicht als Sicherheitsziel für den EVG formuliert. ⇒ A.NK.kein_DoS, A.NK.Ersatzverfahren

Tabelle 3.1: Primäre Werte

3.1.2 Sekundäre Werte

Die sekundären Werte sind in der folgenden Tabelle 3.2 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder 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_WAN

Fortsetzung auf der nächsten Seite

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder erforderliche Annahmen
kryptographisches Schlüsselmaterial (während seiner Speicherung im EVG oder Verwendung durch den EVG)	Vertraulichkeit, Integrität, Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikationspartners sicherzustellen. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz und O.NK.VPN_Auth wirken (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.remote_VPN_Data, T.NK.local_admin_LAN, T.NK.remote_admin_WAN) sowie T.NK.Zert_Prüf
Authentisierungsgeheimnisse (im EVG gespeicherte Referenzdaten und zum EVG übertragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungsgeheimnissen (z. B. Passwort für Administratorauthentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN)
Management-Daten (während ihrer Übertragung zum EVG)	Vertraulichkeit, Integrität, Authentizität	Wenn der EVG administriert wird, dürfen die administrativen Datenströme nicht eingesehen oder unbemerkt verändert werden können. ⇒ alle Bedrohungen, gegen die O.NK.Admin_EVG und OE.NK.Admin_EVG wirken, insbesondere T.NK.local_admin_LAN und T.NK.remote_admin_WAN

Fortsetzung auf der nächsten Seite

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder erforderliche Annahmen
Management-Daten (während ihrer Speicherung im EVG)	Integrität	Management-Daten (z. B. Konfigurationsdaten) des EVG dürfen nicht unbemerkt verändert werden können, da sonst nicht mehr sichergestellt ist, dass der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN)
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. ⇒ alle Bedrohungen, gegen die O.NK.Protokoll wirkt (T.NK.remote_EVG_WAN sowie möglicherweise viele andere auch, abhängig vom Umfang der Protokollierung)

Fortsetzung auf der nächsten Seite

Wert	zu schützende Eigenschaften des Wertes	Erläuterung ⇒ davon abgeleitete Bedrohungen oder erforderliche Annahmen
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, alle Bedrohungen, gegen die O.NK.Zeitdienst wirkt (T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.remote_VPN_Data)
Firmware-Updates	Integrität, Authentizität	Der EVG bietet die Möglichkeit, Daten aus einer (sicheren) Quelle herunterzuladen und nach Prüfung des Urhebers als Firmware-Update zu installieren. ⇒ T.NK.FW, gegen die O.NK.FW wirkt

Tabelle 3.2: 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[2]in Common Criteria v3.1R4 [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 befinden sich die in Tabelle 3.3 aufgeführten Einheiten:

[2]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.

Tabelle 3.3: Externe Entitäten in der Einsatzumgebung des EVGs

Bezeichner	**Erläuterung**
NK	Netzkonnektor (EVG)
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	Client-System
TSL/CRL	Bereitstellungspunkte für TSL und CRL
NK-Admin	(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.

Für den **Leistungserbringer** sind die Leistungen des NK transparent, er arbeitet mit dem Client-System. 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 Client-Systeme 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:

Tabelle 3.4: Betrachtete Objekte

Bezeichner	Erläuterung
CS-Daten	lokal beim Leistungserbringer (in Client-Systemen 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 Abschnitt 3.5: A.NK.sichere_TI). Die Sicherheit der Client-Systeme ist nicht Gegenstand der Betrachtung.

3.3 Bedrohungen

3.3.1 Auswahl der betrachteten Bedrohungen

Der Netzkonnektor muss 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)[3],
- 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 Telematikinfra-struktur-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[4]. 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:

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

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

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

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[5].

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-Daten-SIS anzugreifen, siehe T.NK.remote_VPN_Data); hier sind die Vertraulichkeit und Integrität der übertragenen Daten bedroht.

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

- 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 Administration, die ebenfalls das Ziel von Angriffen sein kann (siehe T.NK.local_admin_LAN).

3.3.2 Liste der Bedrohungen

Ein graphische Darstellung der zu betrachtenden Bedrohungen findet man im Schutzprofil [47], Abbildung 4. Die dort gewählten und erläuterten Bezeichnungen werden auch hier verwendet, jedoch nicht explizit wiederholt. Im Einzelnen werden also folgende Bedrohungen betrachtet:

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

- im Netzkonnektor gespeicherte Geheimnisse in Erfahrung zu bringen (primäre Werte wie *zu schützende Daten der TI und der Bestandsnetze* (siehe Abschnitt 3.1), aber auch sekundäre Werte wie Schlüssel),
- den Netzkonnektor so zu manipulieren, dass zukünftig vertrauliche *zu schützende Daten der TI und der Bestandsnetze* kompromittiert werden können, oder
- den Netzkonnektor so zu manipulieren, dass zukünftig *zu schützende Daten der TI und der Bestandsnetze* 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, 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.

[6] 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.

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 Client-System-Netz in einen unsicheren Systemzustand zu bringen versucht.

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 Client-System zu kompromittieren und möglicherweise im Anschluss daran den Konnektor von dessen LAN-Seite her anzugreifen. Die Kompromittierung eines Client-Systems ist gegeben, wenn ein Angreifer aus dem Transportnetz bzw. dem Internet unautorisiert auf personenbezogene Daten im Client-System zugreifen kann oder wenn der Angreifer ein Client-System erfolgreich und unbemerkt manipulieren kann.

Hierzu werden in Abbildung 4 des Schutzprofiles [47] 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[7] zwischen WAN und LAN leistet.

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 4 aus [47]) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 4 aus [47]) 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 Client-System übertragene Daten zu erhalten.
- Ein Angreifer verändert verschlüsselte Daten während der Übertragung unbemerkt.

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:

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

- 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 entfernter 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.

Hinweis: Der EVG unterstützt keine entfernte Administration.

3.3.2.7 T.NK.counterfeit

Ein Angreifer bringt gefälschte Netzkonnektoren in Umlauf, ohne dass dies vom VPN-Konzentrator erkannt wird[8]. Der Angriff kann durch den unbemerkten Austausch eines bereits im Einsatz befindlichen Geräts erfolgen – wozu in der Regel ein Eindringen in die Räumlichkeiten des Leistungserbringer

[8]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.

erforderlich ist – oder bei der Erstauslieferung durchgeführt werden. Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer verfolgt dieselben Ziele wie unter T.NK.local_admin_LAN besprochen.

3.3.2.8 T.NK.Zert_Prüf

Ein Angreifer manipuliert Sperrlisten, die im Rahmen der Gültigkeitsprüfung von Zertifikaten zwischen dem EVG und einem netzbasierten Dienst (siehe OE.NK.PKI) ausgetauscht werden, 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 Verzeichnisdienstes manipulieren oder sich selbst als Verzeichnisdienst 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, um auf dem EVG die Einstellung einer falschen Uhrzeit zu bewirken, oder gibt sich selbst als Zeitdienst aus. 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. Andererseits können gefälschte DNS-Antworten auch beim Internet-Zugriff von Client-Systemen der Leistungserbringer auftreten. In einem solchen Szenario könnte der Angreifer den Zugriff der Client-Systeme auf manipulierte Systeme umleiten, um Client-Systeme mit bösartigem Code zu infizieren, der dann das lokale Netz, den Netzkonnektor und die zu schützenden Werte bedroht.

3.3.2.11 T.NK.FW

Ein Angreifer stellt manipulierte Daten als Firmware-Update entweder im Internet oder an der lokalen Managementschnittstelle zur Verfügung. Nachdem der EVG diese Daten empfangen hat, werden sie als Firmware-Update installiert. Der Angreifer verfügt über hohes Angriffspotential.

3.4 Organisatorische Sicherheitspolitiken

Es werden drei organisatorische Sicherheitspolitiken definiert:

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.

3.5 Annahmen

Es werden die folgenden Annahmen getroffen:

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

A.NK.gSMC-K **Sicherheitsmodul für den EVG (gSMC-K)**
Der EVG hat Zugriff auf ein Sicherheitsmodul (gSMC-K), das sicher mit dem EVG verbunden ist. Sicher bedeutet in diesem Fall, dass das gSMC-K nicht unbemerkt vom EVG getrennt werden kann und dass die Kommunikation zwischen gSMC-K und EVG weder mitgelesen noch manipuliert werden kann. Das 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) [13] 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.

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.

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 den VPN-Tunnel für Dienste nach § 291a SGB V [9] an die zentrale Telematikinfrastruktur-Plattform weitergeleitet werden müssen.

Anmerkung: Da der Netzkonnektor keine Analyse der Inhaltsdaten vornimmt, leitet er alle Inhaltsdaten aus einem korrekten Aufruf ungeachtet der Zulässigkeit des Aufrufs spezifikationsgemäß weiter.

A.NK.CS **Client-System nutzt EVG korrekt**

Die Client-Systeme nutzen die Sicherheitsdienste des EVG über dessen Schnittstellen automatisch. Durch die Art der Aufrufe ist für den EVG jederzeit eindeutig erkennbar, welche Daten über den VPN-Tunnel für Dienste nach § 291a SGB V [9] an die zentrale Telematikinfrastruktur-Plattform weitergeleitet werden müssen.

Anmerkung: Da der Netzkonnektor keine Analyse der Inhaltsdaten vornimmt, leitet er alle Inhaltsdaten aus einem korrekten Aufruf ungeachtet der Zulässigkeit des Aufrufs spezifikationsgemäß weiter.

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 PP Konnektor ORS1 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 den EVG in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

A.NK.Betrieb_CS **Sicherer Betrieb der Client-Systeme**
Der Betreiber der Client-Systeme organisiert diesen Betrieb in sicherer Art und Weise:

- Er setzt nur Client-Systeme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.
- Er administriert die Client-Systeme in sicherer Art und Weise.
- Er trägt die Verantwortung dafür, dass die Client-Systeme 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 Client-Systeme oder andere IT-Systeme im LAN aufgebracht wird.
- Er ist verantwortlich dafür, dass eine Anbindung der Client-Systeme 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 Client-Systeme liegt sowohl beim Leistungserbringer (der z. B. lokal potentiell bösartige Software oder auch potentiell fehlerhafte Updates der Client-System-Software einspielen könnte) als auch beim Client-System-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 in Übereinstimmung mit der Administrator-Dokumentation des EVG durchgeführt werden. Insbesondere ist für diese Tätigkeiten vertrauenswürdiges und ausgebildetes Personal einzusetzen. Die Administratoren halten Authentisierungs-informationen 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. Da Netzkonnektor und Anwendungskonnektor dasselbe gSMC-K nutzen, ist der physische Schutz durch Verbau im gleichen Gehäuse gegeben.

Die logische Zugriffskontrolle wird durch den SMC-Dienst vermittelt, wobei sichergestellt wird, dass die Komponenten des Konnektors nur auf ihr eigenes Schlüsselmaterial zugreifen.

Kapitel 4

Sicherheitsziele

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 Client-Systeme und sich selbst schützen.

4.1.1 Allgemeine Ziele: Schutz und Administration

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.

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 des gSMC-K einen Nachweis seiner Authentizität ermöglichen.
O.NK.Admin_Auth	**Authentisierung des Administrators** Der Netzkonnektor führt eine Authentisierung des Administrators durch.

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

Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: nur Administratoren können administrative Funktionen ausführen.

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

Weil die Administration über die lokale Netzverbindung PS1 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,
- 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,
- Regeln für die Kommunikation zwischen LAN und den Bestandsnetzen.

Hinweis: Der EVG unterstützt keine entfernte Administration.

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

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

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).

O.NK.FW	**Firmware-Update** Der EVG installiert nur geprüfte und als authentisch festgestellte Daten als Firmware-Update. Er setzt das Firmware-Gruppen Konzept für dezentrale Komponenten gemäß [57], Abschnitt 2.5 durch.

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-Konzentrator) und ermöglicht eine Authentifizierung seiner selbst gegenüber dem VPN-Konzentrator in der zentralen Telematikinfrastruktur-Plattform und gegenüber dem Sicheren Internet Service.

Der EVG prüft zertifikatsbasiert die Authentizität der VPN-Konzentratoren.

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

Der EVG sorgt dafür, dass nur solche kryptografischen Algorithmen verwendet werden, die gemäß Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116) (vgl. [14]) mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen gemKrypt noch gültig sind.

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

O.NK.VPN_Vertraul **Schutz der Vertraulichkeit von Daten im VPN-Tunnel**
Der EVG schützt die Vertraulichkeit der Nutzdaten[1] bei der Übertragung von und zu den VPN-Konzentratoren.

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

Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.

O.NK.VPN_Integrität **Integritätsschutz von Daten im VPN-Tunnel**
Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der EVG 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 **Paketfilter zum WAN**
Der EVG schützt sich selbst und andere Konnektorteile vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN). Wenn der Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt, dann schützt der EVG auch die Client-Systeme.

Mit Ausnahme der Kommunikation der Client-Systeme mit den Bestandsnetzen wird grundsätzlich jeder nicht vom Konnektor generierte, direkte Verkehr aus dem LAN in den VPN-Tunnel zur TI ausgeschlossen (vergl. auch § 291a SGB V Dienste). Es werden Angreifer mit hohem Angriffspotential betrachtet.

[1] Der Begriff „Nutzdaten“ schließt in Übereinstimmung mit [47] 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.PF_LAN **Dynamischer Paketfilter zum LAN**
Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN). Es werden Angreifer mit hohem Angriffspotential betrachtet.

Für *zu schützende Daten der TI und der Bestandsnetze* sowie *zu schützende Nutzerdaten* bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Client-Systemen) 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.

O.NK.Stateful **Stateful Packet Inspection (zustandsgesteuerte Paketfilterung)**
Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter.

4.2 Sicherheitsziele für die Einsatzumgebung

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.

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.

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

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

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

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

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 Sitzungsschlüsseln (session keys), die abgeleitet werden von auf dem gSMC-K gespeicherten Geheimnissen (privater Schlüssel) zur Authentisierung beim Aufbau des VPN-Tunnels (kryptographische Identität des EVG, siehe FTP_ITC.1/NK.VPN_TI).

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.

OE.NK.CS **Korrekte Nutzung des Konnektors durch Client-Systeme (oder weitere Systeme im LAN)**
Die Hersteller von Client-Systemen 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.

OE.NK.Admin_EVG **Sichere Administration des Netzkonnektors**
Der Betreiber des Netzkonnektors muss dafür sorgen, dass administrative Tätigkeiten der Administration in Übereinstimmung mit der Administrator-Dokumentation des EVGs durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges und ausgebildetes 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.

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

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

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

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

Die Auskünfte der Public-Key-Infrastruktur werden von der Infrastruktur signiert. Die Infrastruktur soll hoch verfügbar sein.

OE.NK.phys_Schutz **Physischer Schutz des EVG**

Die Sicherheitsmaßnahmen in der Umgebung müssen den Netzkonnektor vor physischem Zugriff Unbefugter schützen. Der Betreiber des Netzkonnektors legt namentlich die autorisierten Personen fest. Sowohl während als auch außerhalb aktiver Datenverarbeitung im Netzkonnektor müssen die Sicherheitsmaßnahmen in der Umgebung sicherstellen, dass ein Diebstahl des Netzkonnektors oder Manipulationen am Netzkonnektor so rechtzeitig erkannt werden, dass die einzuleitenden Maßnahmen größeren Schaden abwehren.

Anmerkung: Netzkonnektor und Anwendungskonnektor sowie das gSMC-K sind im selben Gehäuse verbaut, so dass dieses Umgebungsziel gleichzeitig auf alle drei Konnektorbestandteile wirkt.

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.

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.

OE.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

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

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

OE.NK.Betrieb_CS **Sicherer Betrieb der Client-Systems**

Der Betreiber der Client-Systeme muss diesen Betrieb in sicherer Art und Weise organisieren:

- Er setzt nur Client-Systeme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.
- Er administriert die Client-Systeme in sicherer Art und Weise.
- Er trägt die Verantwortung dafür, dass die Client-Systeme 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 Client-Systeme oder andere IT-Systeme im LAN aufgebracht wird.
- Er ist verantwortlich dafür, dass eine Anbindung der Client-Systeme 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 Client-Systeme liegt sowohl beim Leistungserbringer (der z. B. lokal potentiell bösartige Software oder auch potentiell fehlerhafte Updates der Client-System-Software einspielen könnte) als auch beim Client-System-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.[2]

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[3] 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.

[2]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 Client-Systeme 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 Client-Systemen (OE.NK.Betrieb_CS) gefordert.

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

4.3 Begründungen für die Sicherheitsziele

4.3.1 Abdeckung der Annahmen

In diesem Abschnitt wird gezeigt, dass die Sicherheitsziele für die Umgebung, gekennzeichnet durch OE.NK.*, die definierten Annahmen, gekennzeichnet durch A.NK.* tatsächlich benötigen, um erfüllt zu werden. Die Darstellung erfolgt zunächst in der Tabelle 4.5. Ein Kreuz „**X**"in Tabelle 4.5 bedeutet, dass zur Erfüllung des Zieles, in dessen Spalte das Kreuz steht, die Annahme, in deren Zeile das Kreuz steht, benötigt wird. Die Erklärung erfolgt im Anschluss.

Annahme (A.NK.*)	**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**	**OE.NK.Ersatzverfahren**	**OE.NK.RNG**	**OE.NK.Echtzeituhr**	**OE.NK.Zeitsynchro**	**OE.NK.KeyStorage**	**OE.NK.PKI**	**OE.NK.SIS**
A.NK.phys_Schutz	X															
A.NK.gSMC-K		X														
A.NK.sichere_TI			X													
A.NK.kein_DoS				X												
A.NK.AK					X											
A.NK.CS						X										
A.NK.Betrieb_AK							X									
A.NK.Betrieb_CS								X								
A.NK.Admin_EVG									X							
A.NK.Ersatzverfahren										X						
A.NK.Zugriff_gSMC-K		X					X									

Tabelle 4.5: Abbildung der Sicherheitsziele für die Umgebung auf die Annahmen

Zunächst zeigt sich, dass tatsächlich alle Annahmen benötigt werden, um die Sicherheitsziele für die Umgebung zu erreichen. Die Ziele OE.NK.RNG, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, OE.NK.KeyStorage, OE.NK.PKI und OE.NK.SIS werden zwar nicht auf Annahmen zurückgeführt, jedoch auf Bedrohungen oder organisatorische Sicherheitspolitiken, wie in Abschnitten 4.3.2 und 4.3.3 gezeigt wird.

Bei fast allen der inhaltlich lediglich umformulierten Annahmen (A.NK.*) und Umgebungszielen (OE.NK.*) 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.Ersatzverfahren,

A.NK.Betrieb_CS und A.NK.Admin_EVG 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.Ersatzverfahren, OE.NK.Betrieb_CS und OE.NK.Admin_EVG. Zu jeder dieser Annahmen existiert ein entsprechendes Umgebungsziel.

Als einzige Ausnahme davon wird die Annahme A.NK.Zugriff_gSMC-K für zwei Umgebungsziele benötigt. Sie 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 ein 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, SAK) auf die gSMC-K betrachtet werden.

Laut OE.NK.Betrieb_AK trägt der Betreiber des EVG die Verantwortung dafür, dass die Anwendungskonnektoren 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.

4.3.2 Abwehr der Bedrohungen

Bedrohungen können sowohl durch Sicherheitsziele für den EVG als auch durch Sicherheitsziele für die Umgebung abgedeckt werden. Wiederum wird zunächst tabellarisch dargestellt, wodurch den Bedrohungen entgegengewirkt wird. Anschließend findet man die Begründungen.

Bedrohung (T.NK.*)	**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**	**OE.NK.Ersatzverfahren**	**OE.NK.RNG**	**OE.NK.Echtzeituhr**	**OE.NK.Zeitsynchro**	**OE.NK.KeyStorage**	**OE.NK.PKI**	**OE.NK.SIS**
T.NK.local_EVG_LAN														X		
T.NK.remote_EVG_WAN		X	X								X		X	X	X	
T.NK.remote_EVG_LAN		X	X					X			X		X	X	X	X
T.NK.remote_VPN_Data		X	X		X		X	X		X	X		X	X	X	X
T.NK.local_admin_LAN									X		X			X		
T.NK.remote_admin_WAN									X		X			X		
T.NK.counterfeit	X	X								X						
T.NK.Zert_Prüf															X	
T.NK.TimeSync													X			
T.NK.DNS								X								

Tabelle 4.6: Abbildung der Sicherheitsziele für die Umgebung auf die Bedrohungen

Es folgt nun die Abbildung zwischen Bedrohungen und Zielen für den EVG in tabellarischer Form.

Bedrohung (T.NK.*)	**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**	**O.NK.FW**	**O.NK.Admin_Auth**
T.NK.local_EVG_LAN	X			X							X	X		
T.NK.remote_EVG_WAN	X			X	X	X	X		X	X		X		
T.NK.remote_EVG_LAN	X			X	X	X	X		X	X	X			
T.NK.remote_VPN_Data					X	X	X	X	X					
T.NK.local_admin_LAN	X		X	X										X
T.NK.remote_admin_WAN	X		X	X										X
T.NK.counterfeit		X												
T.NK.Zert_Prüf							X							
T.NK.TimeSync					X				X					
T.NK.DNS						X								
T.NK.FW													X	

Tabelle 4.7: Abbildung der Sicherheitsziele für den EVG auf die Bedrohungen

In den folgenden Unterabschnitten wird der Nachweis geführt, dass die oben formulierten und in den Tabellen 4.6 und 4.7 auf die Bedrohungen abgebildeten Sicherheitsziele geeignet sind, um die Bedrohungen abzuwehren.

4.3.2.1 T.NK.local_EVG_LAN

T.NK.local_EVG_LAN greift den EVG über seine LAN-Schnittstelle an. Der EVG filtert alle Nachrichten, die ihn auf dieser Schnittstelle erreichen, mit Hilfe des LAN-seitigen Paketfilters (O.NK.PF_LAN; mit grundlegender zustandsgesteuerter Filterungs-Funktionalität); dieser schützt den EVG vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer. Der EVG schützt auch den Anwendungskonnektor vor LAN-seitigen Angriffen (O.NK.PF_LAN) und trägt somit zur Abwehr der Bedrohung bei. Der dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse 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.

Die Abwehr von T.NK.local_EVG_LAN wird durch O.NK.Stateful unterstützt, indem sicherheitsrelevante Ereignisse protokolliert werden.

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. Das 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 protokolliert werden (z. B. die letzte vorgenommene Konfigurationsänderung), und von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

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

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. Das 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 dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse protokolliert werden. Konnte ein Client-System bereits kompromittiert werden, so unterstützt auch der LAN-seitige Paketfilter beim Schutz des EVG (O.NK.PF_LAN): Im vorliegenden Fall der Einbox-Lösung schützt der EVG (O.NK.PF_LAN) auch den Anwendungskonnektor vor LAN-seitigen Angriffen und trägt somit zur Abwehr der Bedrohung bei. Der EVG wird – wie bei T.NK.remote_EVG_WAN – unterstützt von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

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

Angriffe aus dem Internet über den VPN-Tunnel vom Sicheren Internet Service (siehe Angriffspfad 3.2 in Abbildung 2) werden duch 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 trägt der LAN-seitige Packetfilter (O.NK.PF_LAN) zum Schutz des LAN und des EVG bei. Konnte ein LAN dennoch komprimittiert werden, schützen die LAN-seitig installierten Maßnahmen zur Erkennung und Schutz vor bösartigem Code (OE.NK.Betrieb_CS) die Client-Systeme und den EVG.

Die Abwehr von T.NK.remote_EVG_LAN wird durch O.NK.Stateful unterstützt, 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).

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). Das 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 Client-Systeme). Der VPN-Client vollzieht die Entschlüsselung von Daten, die ihm ein

VPN-Konzentrator verschlüsselt zugesendet hat. Die Nutzdaten werden beim Senden integritätsgeschützt übertragen und beim Empfang auf ihre Integrität hin überprüft (O.NK.VPN_Integrität), was Manipulationen ausschließt.

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

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

4.3.2.6 T.NK.remote_admin_WAN

T.NK.remote_admin_WAN betrachtet Angriffe im Zusammenhang mit zentraler Administration. Der Unterschied im Angriffspfad zwischen T.NK.remote_admin_WAN und T.NK.local_admin_LAN besteht darin, dass der Angreifer bei T.NK.remote_admin_WAN aus dem Transportnetz heraus versucht, seinen Angriff durchzuführen, während bei T.NK.local_admin_LAN die Angriffsversuche aus dem lokalen Netz heraus durchgeführt werden. Bei der Abwehr sind jedoch die gleichen Mechanismen beteiligt (Zugriffskontrolle, Authentisierung des Administrators, Selbstschutz, Protokollierung), und diese wirken unabhängig vom Ursprungsort des Angriffsversuchs, daher gilt hier sinngemäß das gleiche wie unter T.NK.local_admin_LAN: zur Abwehr tragen die Ziele O.NK.Admin_EVG, O.NK.Admin_Auth, OE.NK.Admin_EVG, OE.NK.RNG, O.NK.Protokoll, O.NK.Schutz und OE.NK.KeyStorage bei.

Hinweis: Der EVG unterstützt keine entfernte Administration.

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 (O.NK.EVG_Authenticity) einen Nachweis seiner Authentizität , 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 abgewehrt. OE.NK.PKI unterstützt, indem die Gegenseite die Antwort auf die Anfragen signiert zurücksendet.

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 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 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.

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[4]. Der Netzkonnektor löst die öffentlichen Adressen der VPN-Konzentratoren mittels

[4]Für Namensauflüsungen innerhalb der TI und der darin angeschlossenen Netzwerke stellt die TI eigene DNS-Server bereit, die vom Transportnetz bzw. Internet nicht erreichbar und zudem durch DNSSEC gesichert sind.

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. 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 Packetfilter des Netzkonnektors erkannt und verhindert werden (O.NK.Stateful). Dies hängt einerseits vom Vorgehen des Angreifers und andererseits von dem Regelwerk des Paketfilters ab. Bei erkanntem Angriff erfolgt ferner ein Eintrag in das Sicherheitsprotokoll (O.NK.Protokoll).

Im Fall einer DNS-Auflösung durch Client-Systeme beim Zugriff auf das Internet führt die Manipulation der DNS-Antwort dazu, dass Client-Systeme auf Seiten umgelenkt werden können, die nicht ihrer ursprünglichen Intention entsprechen. Erfolgt dies vom Benutzer unbemerkt, können bei bösartigen Systemen die Client-Systeme 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 Client-Systemen aber durch Mechanismen auf den Client-Systemen (Einsatz von sicheren Produkten und Virenscannern) erkannt und neutralisiert werden (OE.NK.Betrieb_CS).

4.3.2.11 T.NK.FW

T.NK.FW adressiert alle Aktionen eines Angreifers, den Firmware-Update-Mechanismus des EVGs zu nutzen, um manipulierte Firmware durch den EVG installieren zu lassen. Neben der Bereitstellung eines manipulierten Firmware-Updates muss der Angreifer (i) das manipulierte Firmware-Update an der vorgesehenen Stelle bereitstellen oder (ii) die URL des Firmware-Updates geeignet manipulieren oder (iii) die Namensauflösung der URL geeignet manipulieren oder (iv) das Firmware-Update über die lokale Management-Schnittstelle hochladen. Welchen Weg zur Manipulation der Angreifer auch wählt, wird er nicht erfolgreich sein, denn das Ziel O.NK.FW sorgt dafür, dass für ein Firmware-Update-Paket geprüft wird, ob es integer und authentisch ist. Nur in diesem Fall wird das Datenpaket als Firmware-Update installiert.

4.3.3 Umsetzung der organisatorischen Sicherheitspolitiken

Die nachfolgende Tabelle 4.8 führt die relevanten Sicherheitsziele für den EVG und für die Umgebung auf und zeigt, durch welche organisatorischen Sicherheitspolitiken diese Ziele erreicht werden.

Organisatorische Sicherheitspolitik (OSP.NK.*)	**O.NK.Zeitdienst**	**OE.NK.Echtzeituhr**	**OE.NK.Zeitsynchro**	**OE.NK.SIS**	**O.NK.PF_WAN**	**OE.NK._CS**
OSP.NK.Zeitdienst_EVG_LAN	**X**	**X**	**X**			
OSP.NK.SIS				**X**	**X**	
OSP.NK.BOF					**X**	**X**

Tabelle 4.8: Abbildung der Sicherheitsziele auf die organisatorischen Sicherheitspolitiken

Die Begründungen für die Umsetzung der organisatorischen Sicherheitspolitiken finden sich in den beiden folgenden Unterabschnitten.

4.3.3.1 OSP.NK.Zeitdienst

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

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

4.3.3.2 OSP.NK.SIS

Die Sicherheitspolitik OSP.NK.SIS fordert einen gesicherten Internet-Zugangspunkt, der die damit verbundenen Netze der Benutzer wirksam gegen Angriffe aus dem Internet schützt. 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 O.NK.PF_WAN 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.

Kapitel 5

Definition erweiterter Komponenten

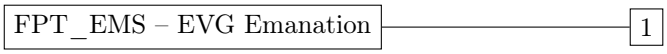
Für die Zwecke dieser Sicherheitsvorgaben wird die Definition einer nicht in den CC, Teil 2 [2] enthaltenen funktionalen Anforderung benötigt, sie sich nicht durch eine Kombination von Anforderungen ausdrücken lässt, die im Teil 2 enthalten sind.

Die Definition ist im Schutzprofil [47] enthalten.

Family FPT_EMS – EVG Emanation

Family behaviour This family defines requirements to mitigate intelligible emanations.

Component levelling:



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 to:	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].

Kapitel 6

Sicherheitsanforderungen

6.1 Notation

Die von den Common Criteria erlaubten Operationen werden wie folgt gekennzeichnet:

- Eine *Verfeinerung* wird durch **fettgedruckten Text** in der Anforderung hervorgehoben und im Bedarfsfall näher erläutert. Gelöschter Text wird ~~durchgestrichen~~ dargestellt.
- Eine *Auswahl* wird durch unterstrichenen Text in der Anforderung hervorgehoben. Der Originaltext findet sich in [2] und wird daher hier nicht wiederholt.
- Eine *Zuweisung* wird ebenfalls durch unterstrichenen Text in der Anforderung hervorgehoben. Der Originaltext findet sich in [2] und wird daher hier nicht wiederholt.
- Eine *Iteration* wird durch einen Schrägstrich „/“ und den Iterationsidentifikator hinter dem Komponentenidentifikator angegeben.

Anmerkung: Die Zulässigkeit der Art und Weise, in der die o. g. Operationen ausgeführt wurden, unterliegt der Evaluierung. Die Tatsache, dass das Schutzprofil [47] zertifiziert ist, bedeutet, dass alle bereits dort vollständig ausgeführten Operationen zulässig sind. Die Zertifizierung des in diesen Sicherheitsvorgabenidentifizierten EVGs bedeutet, dass alle in diesen Sicherheitsvorgabenausgeführten Operationen zulässig sind.

6.2 Funktionale Sicherheitsanforderungen an den EVG

Die funktionalen Sicherheitsanforderungen werden im Folgenden 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.

Die Verwendung von Suffixen folgt den Konventionen aus dem Schutzprofil [47]: 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 diesen Sicherheitsvorgabenwurde zudem das Suffix „NK“ verwendet, selbst wenn keine Iteration vorliegt. Das wurde zur Vereinfachung im Umgang mit der vorgesehenen Composite-Evaluierung des Konnektors ORS1 eingeführt, bei der diese Sicherheitsvorgaben referenziert werden.

6.2.1 VPN-Client

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** that is logically distinct from other communication channels and provides assured identification of its end points **using DNSSEC and certificate based authentication** and protection of the channel data from modification **and** disclosure.
FTP_ITC.1.2/NK.VPN_TI	The TSF shall permit the TSF 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.

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

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

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

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

Dependencies:	No dependencies.
FTP_ITC.1.1/NK.VPN_SIS	The TSF shall provide a communication channel between itself and another trusted IT product **Sicherer Internet Service (SIS)** that is logically distinct from other communicationchannels and provides assured identification of its end points **using DNSSEC and certificate based authentication** and protection of the channel data from modification **and** disclosure.
FTP_ITC.1.2/NK.VPN_SIS	The TSF shall permit the TSF 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.

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.

6.2.2 Dynamischer Paketfilter mit zustandsgesteuerter Filterung

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.

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) on the subjects: (a) IAG, (b) VPN concentrator of the TI, (c) VPN concentrator of the SIS, (d) the TI services, (e) application connector (except the service modules), (f) the service modules (German: Fachmodule) running on the application connector, (g) active entity in the LAN, (h) CRL download server, (i) download server for IANA DNSSEC root keys, (j) hash&URL server, (k) registration server of the VPN network provider, (l) remote management server, the information a) incoming information flows b) outgoing information flows and the operations a) receiving data, b) sending data, c) communicate (i.e. sending and receiving data)
Interpretationshinweise FDP_IFC.1.1/ NK.PF, (l)	Der EVG verwendet das in der Kommunikationsregel angegebene Subjekt „remote management server“ nicht.

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

Tabelle 6.2: Kommunikationsbeziehungen des EVGs

IP-Adressbereich	**Instanz für Kommunikation mit dem Konnektor**
ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der WAN-Adapter des Konnektors angeschlossen ist.
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der LAN-Adapter des Konnektors angeschlossen ist.
ANLW_LEKTR_INTRANET_ROUTES	Adressbereich des Intranet-VPN des LE
NET_SIS	VPN-Konzentratoren der SIS
NET_TI_ZENTRAL	Zentrale Dienste der TI
NET_TI_DEZENTRAL	Adressbereich den 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
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
DNS_ROOT_ANCHOR_URL	IP-Adresse des Download-Servers für die IANA DNSSEC Root Keys
hash&URL-Server	IP-Adresse des hash&URL-Servers
registration server	IP-Adresse des Registrierungsservers

Erläuterungen: Der EVG kommuniziert u.a. mit Endpunkten, die über das Transportnetz (Internet) erreichbar sind. Die Kommunikation erfolgt in diesen Fällen, bevor ein VPN-Tunnel zur TI oder ins Internet über den SIS aufgebaut wurde. Die Kommunikation mit diesen Endpunkten ist eine Voraussetzung für den späteren Aufbau einer VPN-gesicherten Verbindung. Diese Endpunkte sind die IP-Adresse

des CRL-Download-Servers[1], die IP-Adresse des Download-Servers der IANA DNSSEC Root-Keys[2], der DNS-Server zur Auflösung gegebener FQDNs in IP-Adressen, der Hash-&URL-Server und der Registrierungsserver[3]. Die Kommunikation mit dem Registrierungsserver ist erforderlich, um das auf der gSMC-K befindliche Authentisierungszertifikat des EVGs für Authentisierung gegenüber dem VPN-Konzentrator der TI zu aktivieren. Die Kommunikation mit dem Download-Server der IANA DNSSEC Root-Keys ist erforderlich, um DNSSEC-Antworten korrekt zu validieren. Der CRL-Download-Server stellt Sperrlisten für zurückgezogene Authentisierungszertifikate von VPN-Konzentratoren zur Verfügung, der Hash&-URL-Server wird kontaktiert, wenn der VPN-Client diesen Modus[4]zum Austausch der Authentisierungszertifikate mit dem VPN-Konzentrator verwenden soll.

Hinweis: Tabelle 6.2 wurde aus dem Schutzprofil übernommen. Es fehlt dort der Eintrag für den DNS-Server. Administratoren des EVGs können den zur Auflösung der IP-Adresse des zu nutzenden VPN-Konzentrators verwendenden DNS-Server konfigurieren. Gemäß [16] verwaltet der EVG in der Variable DNS_SERVERS_INT[5]eine Liste von DNS-Servern im Transportnetz, die dafür Aufgabe zu verwenden sind.

Hinweis: In den SFRs der Paketfilterregeln wird die Bezeichnung ANLW_FW_SIS_ADMIN_RULES benutzt. Diese Variable ist eine Liste einschränkender Filterregeln, die vom Administrator des EVGs definiert werden können und ausschließlich im SIS-Tunnel aktiv sind (siehe dazu [16], Anhang E).

Hinweis: Für den EVG existiert keine Remote-Management-Lösung und kein Remote-Management-Server.

Tabelle 6.3: IP-Adressen des Konnektors

IP-Adressen des Konnektors	Erläuterung
ANLW_LAN_IP_ADDRESS	LAN-seitige Adresse des EVG, unter dieser Adresse werden die Dienste des Konnektors 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 den IAG werden folgende Sicherheitsattribute definiert:

[1] CERT_CRL_DOWNLOAD_ADDRESS
[2] DNS_ROOT_ANCHOR_URL
[3] *registration server*
[4] Der EVG erlaubt die Aktivierung des Modus *Hash&-URL* über die Administrationsoberfläche.
[5] Siehe [16], TAB_KON_654.

Tabelle 6.4: Sicherheitsattribute des IAG

Sicherheitsattribut	Erläuterung
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.
ANLW_ANBINDUNGS_MODUS	Adressbereich der WAN-Schnittstellen der Konnektoren für die Kommunikation mit der TI oder den Bestandsnetzen
ANLW_INTERNET_MODUS	WAN-seitige Adresse des EVG

Hinweis zur Interpretation: Die Betriebsparameter ANLW_ANBINDUNGS_MODUS und ANLW_INTERNET_MODUS sind Parameter des EVGs und nicht des IAGs. Die Belegung dieser Parameter mit konkreten Werten beeinflusst jedoch die Nutzung des IAGs durch den EVG. In gleicher Weise wird in FDP_IFF.1.1/NK.PF die Zuweisung ebenjener Sicherheitsattribute zum IAG interpretiert.

Hinweis zu Tabelle 6.4: Im Schutzprofil lautet die Beschriftung dieser Spalte „IP-Adressen des Konnektors“ . Offensichtlich handelt es sich bei den dargestellten Parametern nicht um IP-Adressen des Konnektors, sondern um die IAG-IP-Adresse, Anbindungsmodus und Internet-Modus. Die aus dem Schutzprofil übernommene Beschreibung von ANLW_ANBINDUGS_MODUS und ANLW_INTERNET_MODUS ist nicht korrekt. Es handelt sich in beiden Fällen um die in Abschnitt 1.3.4 angegebenen Betriebsparameter.

Hinweis zu den Paketfilterregeln: Die SFRs FDP_IFF.1.1/NK.PF bis FDP_IFF.1.5/NK.PF definieren die vom EVG durchzusetzenden Paketfilterregeln. Dabei ist zu beachten, dass solche Regeln, die sich auf die Kommunikation zur TI oder zum SIS beziehen voraussetzen, dass ein entsprechender VPN-Tunnel besteht und aktiv ist. Ist der betreffende Tunnel nicht vorhanden, so kommen die Kommunikationsregeln auch nicht zur Anwendung bzw. sämtliche Kommunikation, die innerhalb dieser Tunnel erlaubt ist, ist dann nicht erlaubt.

Hinweis zu verwendeten Begriffen: In SFRs werden englische Übersetzungen der ursprünglichen deutschen Begriffe genutzt. Das Subjekt „connector“ wird im Zusammenhang mit der jeweiligen SFR mit einer Interpretation versehen, da es sich sowohl um den EVG als auch den Anwendungskonnektor oder den Gesamtkonnektor handeln kann. Der Begriff „service module “ meint Fachmodule. Der Begriff „application connector“ meint den Anwendungskonnektor.

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 based on the following types of subject and information security attributes: (1) IP address, (2) port number, (3) protocol type, (4) direction (inbound and outbound IP[6] traffic) The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES. The subject IAG has the security attributes (1) ANLW_IAG_ADDRESS, (2) ANLW_ANBINDUNGS_MODUS, (3) ANLW_INTERNET_MODUS[7].
Interpretationshinweis FDP_IFF.1.1/NK.PF:	FDP_IFF.1.1/NK.PF: Es gilt die Interpretation der IAG-Sicherheitsattribute gemäß vorliegender Erläuterungen zu Tabelle 6.4.

[6] IP = Internet Protocol

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

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 the 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 and

b) to sent packetes with destination IP address VPN_KONZENTRATOR_TI_IP_ADDRESS and to receive packets with destination 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 or a service module 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 and

b) to sent packetes with destination IP address VPN_KONZENTRATOR_SIS_IP_ADDRESS and to receive packets with destination 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 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 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 entities in the LAN if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=IAG und ANLW_IAG_ADDRESS ≠ ““).

(14) The TSF shall redirect communication from entities in LAN to default gateways if (ANLW_INTERNET_MODUS=IAG und ANLW_IAG_ADDRESS ≠ ““ and MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled)[8].

Interpretationshinweise FDP_IFF.1.2/NK.PF, (4)

FDP_IFF.1.2/NK.PF, (4): Im Modus *InReihe* wird die Adresse ANLW_WAN_IP_ADDRESS auf den WAN-Adapter abgebildet. Gemäß Konnektorspezifikation [16] ist diese Adresse fest auf den WAN-Adapter gebunden. Abweichend davon wird der Modus *Parallel* so ausgelegt, dass diese Adresse identisch mit ANLW_LAN_IP_ADDRESS ist und die FDP_IFF.1.2/NK (4) entsprechend gilt.

Das in der Kommunikationsregel angegebene Subjekt „connector“ meint den EVG, da die Kommunikationsdienste von diesem erbracht werden.

FDP_IFF.1.2/NK.PF, (4c): Für den EVG existiert kein *remote management server*. Die Kommunikation mit der Entität „registration server“ erfolgt ebenso wie die zyklische Kommunikation mit dem CRL-Downloadserver durch den Anwendungskonnektor.

FDP_IFF.1.2/NK.PF, (4d): Der EVG unterstützt DNS sowohl per UDP als auch per TCP. Dementsprechend ist die Kommunikation für beide Varianten erlaubt.

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

Interpretationshinweise FDP_IFF.1.2/NK.PF, (5)	FDP_IFF.1.2/NK, (5): Das Subjekt „connector“ meint sowohl den EVG als auch den Anwendungskonnektor. Die Regel wird so interpretiert, dass aktive Komponenten aus dem Netz des Leistungserbringers sowohl die vom EVG angebotenen Dienste wie DHCP und NTP, Vermittlung des Datenverkehrs ins Internet über SIS, den Zugriff auf die Management-Schnittstelle als auch die vom AK angebotenen SOAP-Dienste nutzen können (vgl. dazu Abschnitt 1.3.5). Die Firewall-Regeln erlauben den Zugriff auf diese Dienste explizit. Es ist zu beachten, dass auch [16] den Begriff „Basisdienst“ nicht eindeutig definiert und diesen wechselseitig sowohl für Dienste des Netz- als auch des Anwendungskonnektors benutzt. Für die Interpretation der Firewallregel ist dies jedoch unschädlich, da keine weitere Unterscheidung erforderlich ist, ob der Dienst vom EVG oder dem Anwendungskonnektor erbracht wird.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (6)	FDP_IFF.1.2/NK, (6): Die Regel wird so interpretiert, dass der Anwendungskonnektor sowohl eingehende Kommunikation aus dem Netz des Leistungserbringers und erreichbarer Subnetze annehmen als auch eigenständig in diese Netze kommunizieren darf. Dies ist wenigstens beim cetp-Protokoll gemäß [16] erforderlich.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (7b)	FDP_IFF.1.2/NK.PF, (7b): Anders als im Text der SFR angegeben, empfängt der EVG Pakete mit Quelladresse (source address) VPN_KONZENTRATOR_TI_IP_ADDRESS.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (8)	FDP_IFF.1.2/NK.PF, (8): Die angegebenen Kommunikationsregeln setzen voraus, dass der Betriebsparameter MGM_LU_ONLINE=Enabled und der VPN-Tunnel in die TI aufgebaut wurde. Die angegebene Kommunikation ist ohne aufgebauten VPN-Tunnel in die TI nicht zulässig und wird vom EVG unterbunden. Im Zusammenhang mit FDP_IFF.1.2/NK.PF, (8f) wird das DNS-Protokoll vom EVG genutzt. D.h. die Regel erlaubt dem EVG die Kommunikation unter Verwendung des DNS-Protokolls mit dem Segment DNS_SERVERS_BESTANDSNETZE.

Interpretationshinweise FDP_IFF.1.2/NK.PF, (9b)	FDP_IFF.1.2/NK.PF, (9b): Anders als im Text der SFR angegeben, empfängt der EVG Pakete mit Quelladresse (source address) VPN_KONZENTRATOR_SIS_IP_ADDRESS.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (10)	FDP_IFF.1.2/NK.PF, (10): Sinngemäß ist mit dieser SFR die Gematik Anforderung TIP1-A_4734 gemeint, die besagt, dass Pakete mit Quelladresse im Segment NET_SIS vom EVG nur ausgehend von VPN-Konzentratoren des SIS empfangen werden dürfen.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (11)	FDP_IFF.1.2/NK.PF, (11): Die angegebenen Kommunikationsregeln setzen voraus, dass der Betriebsparameter ANLW_INTERNET_MODUS=SIS und ein VPN-Tunnel zum SIS aufgebaut wurde. Andernfalls unterbindet der EVG die angegebene Kommunikation.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (11a)	FDP_IFF.1.2/NK.PF, (11a): Das Subjekt „connector “ wird als EVG interpretiert.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (11b)	FDP_IFF.1.2/NK.PF, (11b): Der Betriebsparameter ANLW_FW_SIS_ADMIN_RULES meint die vom Administrator des EVGs erweiterbaren Firewall-Regeln des EVGs für den SIS.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (12)	FDP_IFF.1.2/NK.PF, (12): Der EVG setzt RFC 1812, Abschnitt 4.3.3.2 um und sendet ein ICMP Redirect Paket.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (13)	FDP_IFF.1.2/NK.PF, (13): Der EVG setzt RFC 1812, Abschnitt 4.3.3.2 um und sendet ein ICMP Redirect Paket.
Interpretationshinweise FDP_IFF.1.2/NK.PF, (14)	FDP_IFF.1.2/NK.PF, (14): Der EVG kann sich wie ein RFC 1812-konformer Router verhalten. Die angegebene Regel wird so interpretiert, dass der EVG unter den genannten Bedingungen zu routende Pakete an den IAG verweisen soll.

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 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[9].

Interpretationshinweise FDP_IFF.1.3/NK.PF

FDP_IFF.1.3/NK.PF: Satz 1) Der Betriebsparameter ANLW_FW_SIS_ADMIN_RULES meint die vom Administrator des EVGs erweiterbaren Firewall-Regeln des EVGs für den SIS.
Satz 2) Diese Regel wird so interpretiert, dass der EVG mit Ausnahme derjenigen Kommunikation, die zum Aufbau der VPN-Tunnel erforderlich ist, keinerlei Kommunikation mit dem WAN betreibt, die nicht IPsec-gesichert ist.

FDP_IFF.1.4/NK.PF

The TSF shall explicitly authorise an information flow based on the following rules: Stateful Packet Inspection[10].

[9] assignment: additional information flow control SFP rules

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

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 (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).

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

Erläuterung: Die in Übereinstimmung mit den Zielen O.NK.PF_WAN und O.NK.PF_LAN zu erreichende dynamische Paketfilterung wird durch FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF gefordert.[11]

Interpretationshinweise FDP_IFF.1.5/NK.PF (2) FDP_IFF.1.5/NK.PF (2): Die Kommunikationsregel wird so gedeutet, dass keine Kommunikation mit dem Internet erlaubt sein soll. Da diese über den SIS erfolgt, wird in der angegebenen Kommunikationsregel eben jener Terminus verwendet.

[11]Die Anforderungen FDP_ITC.1/NK.PF und FDP_IFF.1/NK.PF sorgen dafür, dass die Ziele O.NK.PF_WAN und O.NK.PF_LAN (dynamische Paketfilterung) erreicht werden.

Interpretationshinweise FDP_IFF.1.5/NK.PF (8)	FDP_IFF.1.5/NK.PF (8): Die SFR wird wie folgend korrigiert: The TSF prevents communication with the Internet via SIS initiated by entities in LAN if MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=KEINER.
Interpretationshinweise FDP_IFF.1.5/NK.PF (9)	FDP_IFF.1.5/NK.PF (9): Die TSF setzen durch, dass keine Kommunikation aus dem VPN-Tunnel zum SIS zum VPN-Tunnel der TI möglich ist.
Interpretationshinweise FDP_IFF.1.5/NK.PF (10)	FDP_IFF.1.5/NK.PF (10): Die Regel wird so interpretiert, dass der EVG sämtliche Kommunikation mit dem Weitverkehrsnetz über den LAN-Adapter unterbindet, sofern der Betriebsparameter ANLW_WAN_ADAPTER_MODUS=ACTIVE gesetzt ist und der EVG daher im Modus *InReihe* betrieben wird.
Interpretationshinweise FDP_IFF.1.5/NK.PF (11)	FDP_IFF.1.5/NK.PF (10): Die Regel wird so interpretiert, dass der EVG sämtliche Kommunikation mit dem Weitverkehrsnetz über den WAN-Adapter unterbindet, sofern der Betriebsparameter ANLW_WAN_ADAPTER_MODUS=DISABLED gesetzt ist und der EVG daher im Modus *Parallel* betrieben wird.

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).

FMT_MSA.3/NK.PF Static attribute initialisation

	Restriktive Paketfilter-Regeln
Dependencies:	FMT_SMR.1 Security roles hier erfüllt durch: FMT_SMR.1/NK FMT_MSA.1 Management of security attributes hier erfüllt durch: FMT_MSA.1/NK.PF
FMT_MSA.3.1/NK.PF	The TSF shall enforce the PF_SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/NK.PF	The TSF shall allow the administrator to specify alternative initial values to override the default values when an object or information is created.
Refinement:	Bei den Sicherheitsattributen handelt es sich um die Filterregeln für den dynamischen Paketfilter (FDP_IFF.1.2/NK.PF). Restriktiv 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.
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 diskutiert.

6.2.3 Netzdienste

Zeitsynchronisation

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

FPT_STM.1/NK Reliable time stamps

	Der EVG stellt verlässliche Zeitstempel bereit, indem er die Echtzeituhr gemäß OE.NK.Echtzeituhr regelmäßig synchronisiert.
Dependencies:	No dependencies.
FPT_STM.1.1/NK	The TSF shall be able to provide reliable time stamps.
Refinement:	Die Zuverlässigkeit (*reliable*) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [23] erreicht. Der EVG verwendet den verlässlichen Zeitstempel für sich selbst und bietet anderen Konnektorteilen eine Schnittstelle zur Nutzung des verlässlichen Zeitstempels an. Befindet sich der EVG im Online-Modus, muss er die Zeitsynchronisation mindestens bei Start-up, einmal innerhalb von 24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht *nicht mehr als 330 ms* von der Zeitinformation der darüberliegenden Stratum-Ebene ab. Der EVG signalisiert der Einsatzumgebung durch eine Signaleinrichtung (genauer: eine LED und zwei 7-Segment Anzeigen), wenn ein kritischer Betriebszustand (hier: eine nicht korrigierbare Zeitabweichung größer als 330 ms) erreicht ist.

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[12] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/NK.Zert	The TSF shall use interpretation rules 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. Außerdem muss der EVG überprüfen, dass die zur Authentisierung und im Zertifikat verwendeten Algorithmen gemäß *Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116)* [14] noch zulässig sind.

[12] assignment:list of TSF data types

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.

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 the following objects: cryptographic keys (and session keys) used for the VPN, sensitive user data (zu schützende Daten der TI und der Bestandsnetze and zu schützende Nutzerdaten).
Refinement:	Die sensitive 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.

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 during initial start-up and at the request of the administrator to demonstrate the correct operation of the TSF.
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3/NK	The TSF shall provide authorised users with the capability to verify the integrity of the TSF.
Refinement:	Zur Erfüllung der Anforderungen aus FPT_TST.1/NK muss der EVG folgende Mechanismen implementieren: • die Prüfung kryptographischer Verfahren bei Programmstart, • die Prüfung des statischen Kernels (Signaturprüfung), • die Prüfung der Signaturen vorhandener (vom Hersteller angepasster) SW-Komponenten im Netzkonnektor.

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 3.2 in Abschnitt 3.1.2). Zur Definition der Anforderung FPT_EMS.1/NK siehe Kapitel 5.

Der private Authentisierungsschlüssel für das VPN wird bereits durch das gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG soll darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll verhindern, etwa die mit Hilfe des gSMC-K abgeleiteten 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) in excess of limits that ensure that no leakage of this sensitive data occurs enabling access to • session keys derived from private VPN authentication keys, and • data to be protected (zu schützende Daten der TI und der Bestandsnetze).
FPT_EMS.1.2/NK	The TSF shall ensure attackers on the transport network (WAN) or on the local network (LAN) are unable to use the following interface WAN interface or LAN interface of the connector to gain access to the sensitive data (TSF data and user data) listed above.

Sicherheits-Log

Der EVG führt ein Sicherheits-Log wie unter Sicherheitsdienst Protokollierung in Abschnitt 1.3.5 beschrieben. Vergleiche dazu auch die Konnektor-Spezifikation [16], 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:

a) All auditable events for the minimum level of audit; and

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

Refinement: Der in CC angegebene *auditable event a) Start-up and shut-down 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 ~~(if applicable)~~, and the outcome (success or failure) of the event; and

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

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.

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 und FMT_SMR.1/NK), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten (FMT_MTD.1/NK) ausführen darf. Die Authentisierung erfolgt durch den EVG (siehe O.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 (siehe oben: FDP_IFC.1/NK.PF) für den dynamischen Paketfilter 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.
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.

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 change_default, query, modify, delete, clear the real time clock and packet filtering rules to the role Administrator.
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.

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) 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.

FTP_TRP.1/NK.Admin Trusted path

	Trusted Path für den Administrator.
Dependencies:	No dependencies.
FTP_TRP.1.1/NK.Admin	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification.
FTP_TRP.1.2/NK.Admin	The TSF shall permit local 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.

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.)

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 to restrict the ability to query, modify, delete the security attributes packet filtering rules to the role Administrator.

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

1. 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
2. die Kommunikation zwischen dem LAN einerseits und dem Transportnetz, der Telematikinfrastruktur sowohl gesicherte als auch offene Fachdienste und zentrale Dienste, bzw. den Bestandsnetzen (außer Freischalten aktiver Bestandsnetze) andererseits

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

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

FIA_UAU.1/NK Timing of authentication

Dependencies	FIA_UID.1 Timing of identification, hier erfüllt durch FIA_UID.1/NK.SMR
Hierarchical to:	No other components
FIA_UAU.1.1/NK	The TSF shall allow all actions except for administrative actions (as specified by FMT_SMF.1/NK) on behalf of the user to be performed before the user is authenticated
FIA_UAU.1.2/NK	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user

FIA_UAU.5/NK Multiple authentication mechanisms

Verwendete Authentisierungsverfahren

FIA_UAU.5.1/NK The TSF shall provide

1. Rule 1: username / password authentication
2. Rule 2: certificate authenticated trusted path

to support user authentication.

FIA_UAU.5.2/NK The TSF shall authenticate any user's claimed identity according to the

1. Regel 1 (Rule 1) wird auf der LAN-Seite (LAN-Schnittstelle) durchgesetzt. Die Autorisierung eines Administrators aus dem Netz des Leistungserbringers verlangt die Angabe von Nutzername und Passwort zur Authentisierung. Aus dem Netz des Leistungserbringers können ausschließlich lokale Administratoren und Super-Administratoren authentisiert und demzufolge autorisiert werden. Authentisierungsversuche von Remote-Administratoren werden abgewiesen.

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.

Subjekt	Sicherheitsattribut	Möglicher Wert
Administrator	Autorisierungsstatus	autorisiert nicht autorisiert

Hinweis:	Der EVG setzt die Authentisierung des Administrators eigenständig durch. Aus diesem Grunde wurde OE.NK.Admin_Auth in ein Sicherheitsziel des EVGs umgewandelt.

6.2.7 Kryptographische Basisdienste

Der Konnektor soll laut Dokument „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“ [18] die im Folgenden aufgelisteten kryptographischen Primitive implementieren.

FCS_COP.1/NK.Hash Cryptographic operation	
	Zu unterstützende Hash-Algorithmen
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction Alle bisher für FCS_COP.1/NK.Hash genannten Abhängigkeiten werden nicht erfüllt. Begründung: Bei einem Hash-Algorithmus handelt es sich um einen kryptographischen Algorithmus, der keine kryptographischen Schlüssel verwendet. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels und zu seiner Zerstörung erforderlich.
FCS_COP.1.1/NK.Hash	The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and cryptographic key sizes [none] that meet the following: FIPS PUB 180-4 [26].

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 in accordance with a specified cryptographic algorithm HMAC with SHA-1, SHA-256, SHA-384, SHA-512 and cryptographic key sizes of at least 32 bytes that meet the following: FIPS PUB 180-4 [26], RFC 2404 [40], RFC 4868 [41], RFC 7296 [48].

FCS_COP.1/NK.Auth Cryptographic operation

	Authentisierungs-Algorithmen, die im Rahmen von Authentisierungsprotokollen zum Einsatz kommen
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] 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.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

in accordance with a specified cryptographic algorithm sha256withRSAEncryption OID 1.2.840.113549.1.1.11 and cryptographic key sizes 2048 bit that meet the following: RFC 3447 (PKCS#1) [25], FIPS PUB 180-4 [26]

FCS_COP.1/NK.FWAuth Cryptographic operation

Authentisierungs-Algorithmen, die im Rahmen des Firmware-Updates 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

FCS_CKM.4 Cryptographic key destruction: nicht erfüllt

Begründung der Nicht-Erfüllung der Abhängigkeit FCS_CKM.4: Der EVG importiert einen öffentlichen Schlüssel aus dem Sicherheitsmodul gSMC-K. Ein explizites Überschreiben dieses Schlüssels ist zur Erbringung der Sicherheitsleistungen des EVGs nicht erforderlich.

FCS_COP.1.1/NK.FWAuth The TSF shall perform

a) verification of digital signatures

in accordance with a specified cryptographic algorithm sha256withRSAEncryption OID 1.2.840.113549.1.1.11 and cryptographic key sizes 2048 bit, 4096 bit that meet the following: RFC 3447 (PKCS#1) [25], FIPS PUB 180-4 [26]

FCS_COP.1/NK.ESP Cryptographic operation

	Zu unterstützende Verschlüsselungs-Algorithmen für die IPsec-Tunnel gemäß den Anforderungen 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 in accordance with a specified cryptographic algorithm AES-CBC (OID 2.16.840.1.101.3.4.1.42) and cryptographic key sizes 256 bit that meet the following: FIPS 197 [28], RFC 3602 [39], RFC 4303 (ESP) [34], specification [18].

FCS_COP.1/NK.IPsec Cryptographic operation

	Zu unterstützende Verschlüsselungs-Algorithmen für die IPsec-Tunnel gemäß den Anforderungen 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 in accordance with a specified cryptographic algorithm IPsec-protocol and cryptographic key sizes 256 bit that meet the following: RFC 4301 (IPsec) [31], specification [18].

FCS_CKM.1/NK Cryptographic key generation

Dependencies:	[FCS_CKM.2 Cryptographic key distribution oder FCS_COP.1 Cryptographic operation] hier erfüllt durch die vorstehend genannten Anforderungen FCS_COP.1/NK.Hash, FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec und FCS_CKM.2/NK.IKE 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 Schlüsselerzeugung auf der Basis von Zufallszahlen mit hinreichender Entropie für AES and specified cryptographic key sizes AES: 256 Bit that meet the following: specification [18], BSI-TR-03116 [14].

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 that meets the following standard: diffie-hellman group 14 from RFC 3526 [42], RFC 7296 [48], specification [18], TR-02102-3 [15].

FCS_CKM.4/NK Cryptographic key destruction

	Löschen nicht mehr benötigter Schlüssel.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FCS_CKM.1/NK
FCS_CKM.4.1/NK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method durch byteweises Überschreiben mit dem festen Wert 0x00 that meets the following: none.

6.2.8 Firmware-Update

Der EVG setzt gemäß [57], Abschnitt 2.5 das Firmwaregruppenkonzept für dezentrale Komponenten durch.

FDP_ACC.1/NK.FWUpdate Subset access control

	Teilweise Zugriffskontrolle beim Firmware-Update
Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control, hier erfüllt durch FDP_ACF.1/NK.FWUpdate
FDP_ACC.1.1/NK.FWUpdate	The TSF shall enforce the Firmware-Update SFP on 1. subjects: Administrators 2. objects: Firmware-Update 3. actions: Firmware-Update installation

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

	Zugriffskontrolle auf Basis von Sicherheitsattributen beim Firmware-Update
Hierarchical to:	No other components

Dependencies:	FDP_ACC.1, erfüllt durch FDP_ACC.1/NK.FWUpdate FMT_MSA.3, nicht erfüllt, da keine Sicherheitsattribute verwaltet werden
FDP_ACF.1.1/NK.FWUpdate	The TSF shall enforce the Firmware-Update SFP to objects based on the following: • Subjekte: Administrator • Objekte: Firmware-Update Paket mit den Sicherheitsattributen: Signatur und Liste erlaubter Firmware-Versionen (Firmwaregruppe)
FDP_ACF.1.2/NK.FWUpdate	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Der EVG soll nur dann eine Aktualsierung der Firmware vornehmen, wenn: • Die Signatur des Firmware-Updates kann erfolgreich verifiziert werden • Die Version der zu installierenden Firmware ist eine erlaubte Firmware-Version gemäß der Liste erlaubter Firmware-Versionen • Es erfolgt kein Downgrade der Firmware-Gruppe
FDP_ACF.1.3/NK.FWUpdate	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/NK.FWUpdate	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: Der EVG soll die Installation des Firmware-Updates nur nach ausdrücklicher Einwilligung durch den Administrator vornehmen.

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

Import von Benutzerdaten ohne Sicherheitsattribute

Hierarchical to:	No other components.

Dependencies:	[FDP_ACC.1, or FDP_IFC.1], erfüllt durch by FDP_ACC.1/NK.FWUpdate FMT_MSA.3, nicht erfüllt, da keine Sicherheitsattribute verwaltet werden müssen.
FDP_ITC.1.1/NK.FWUpdate	The TSF shall enforce the Firmware-Update SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2/NK.FWUpdate	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3/NK.FWUpdate	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: 1. Die TSF sollen die Integrität und Authentizität des Firmware-Update Pakets vor der Ausführung des Update-Vorgangs verifizieren. 2. Der EVG übernimmt die im Firmware-Update Paket angegebene Firmware-Gruppe, sofern diese eine höhere Version als die aktuelle ausweist 3. Ein Wechsel ist zu jeder Firmware-Version der aktuellen Firmware-Gruppe erlaubt

6.3 Anforderungen an die Vertrauenswürdigkeit des EVG

Es wird die Vertrauenswürdigkeitsstufe EAL3+ gefordert (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). Daraus ergibt sich eine Resistenz gegen hohes Angriffspotential. Darüber hinaus wird ALC_FLR.2 gefordert. Eine Erklärung für die gewählte EAL-Stufe findet sich in Abschnitt 6.6.

Einige Anforderungen an die Vertrauenswürdigkeit (Assurance) werden wie in den folgenden Unterabschnitten beschrieben verfeinert.

6.3.1 Verfeinerung von ALC_DEL.1

ALC_DEL.1 wird wie folgt verfeinert:

Das Auslieferungsverfahren muss Schutz gegen das In-Umlauf-Bringen gefälschter Konnektoren bieten (sowohl während der Erstauslieferung als auch bedingt durch unbemerkten Austausch), siehe O.NK.EVG_Authenticity. Dies unterstützt die Verwendung der (in EAL3 bereits enthaltenen) Komponente ALC_DEL.1. Das Auslieferungsverfahren muss so ausgestaltet werden, dass das Ziel O.NK.EVG_Authenticity erfüllt wird.

Der Hersteller muss das Auslieferungsverfahren beschreiben. Die Beschreibung des Auslieferungsverfahrens muss zeigen, auf welche Weise das Auslieferungsverfahren (in Verbindung mit den Verfahren zur Inbetriebnahme) des EVGs sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

Der Evaluator muss die Beschreibung analysieren (examine), um festzustellen, dass sie beschreibt, auf welche Weise das Auslieferungsverfahren (in Verbindung mit den Verfahren zur Inbetriebnahme) des EVGs sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

6.3.2 Verfeinerungen von AGD_OPE.1

AGD_OPE.1 wird bzgl. der Inbetriebnahme wie folgt verfeinert:

Das Verfahren zur Inbetriebnahme muss Schutz gegen das In-Umlauf-Bringen gefälschter Konnektoren bieten (sowohl während der Erstauslieferung als auch bedingt durch unbemerkten Austausch), siehe O.NK.EVG_Authenticity. Dies unterstützt die Verwendung der (in EAL3 bereits enthaltenen) Komponente AGD_OPE.1. Das Verfahren zur Inbetriebnahme muss so ausgestaltet werden, dass das Ziel O.NK.EVG_Authenticity erfüllt wird.

Der Hersteller muss in seiner Benutzerdokumentation das Verfahren zur Inbetriebnahme des EVGs beschreiben. Diese Beschreibung muss zeigen, auf welche Weise das Verfahren zur Inbetriebnahme (in Verbindung mit dem Auslieferungsverfahren) sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

Der Evaluator muss die Beschreibung analysieren (examine), um festzustellen, dass sie beschreibt, auf welche Weise das Verfahren zur Inbetriebnahme (in Verbindung mit dem Auslieferungsverfahren) sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

AGD_OPE.1 wird bzgl. der Administration der Paketfilter-Regeln wie folgt verfeinert:

Die Benutzerdokumentation muss für den Administrator verständlich beschreiben, welche Paketfilter-Regeln er administrieren kann. Die Benutzerdokumentation muss den Administrator befähigen, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu konfigurieren. Für die von ihm administrierbaren Paketfilter-Regeln muss er in die Lage versetzt werden, geeignete Regelsätze aufzustellen.

Der Hersteller muss in seiner Benutzerdokumentation beschreiben, welche Paketfilter-Regeln der Administrator administrieren kann. Die Benutzerdokumentation muss den Administrator befähigen, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu konfigurieren. Für die von

ihm administrierbaren Paketfilter-Regeln muss er in die Lage versetzt werden, geeignete Regelsätze aufzustellen.

Der Evaluator muss die Benutzerdokumentation analysieren (examine), um festzustellen, dass sie beschreibt, welche Paketfilter-Regeln der Administrator administrieren kann, und dass sie den Administrator befähigt, die von ihm administrierbaren Paketfilter-Regeln in sicherer Art und Weise zu konfigurieren (Für die von ihm administrierbaren Paketfilter-Regeln muss der Administrator in die Lage versetzt werden, geeignete Regelsätze aufzustellen).

AGD_OPE.1 wird bzgl. der Internet-Anbindung wie folgt verfeinert:

Die Benutzerdokumentation muss die Benutzer und Betreiber des Konnektors über die Risiken aufklären, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. das Internet erfolgt.

Der Hersteller muss in der Benutzerdokumentation die Benutzer und Betreiber des Konnektors über die Risiken aufklären, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. Internet erfolgt. Zudem muss der Hersteller in der Benutzerdokumentation verständlich darauf hinweisen, dass auch Angriffe aus dem Internet über SIS nicht auszuschließen sind. Das Client-System muss entsprechende Sicherheitsmaßnahmen besitzen.

Der Evaluator muss die Benutzerdokumentation analysieren (examine), um festzustellen, dass sie die Benutzer und Betreiber des Konnektors hinreichend gut (verständlich und vollständig) über die Risiken aufklärt, die entstehen, wenn neben dem EVG eine weitere Anbindung des lokalen Netzwerks des Leistungserbringers an das Transportnetz bzw. Internet erfolgt.

6.3.3 Verfeinerung von ADV_ARC.1

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 Update-Mechanismen 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

6.4.1 Abbildung der EVG-Ziele auf Sicherheitsanforderungen

Tabelle 6.35 stellt die Abbildung der EVG-Ziele auf Sicherheitsanforderungen zunächst tabellarisch im Überblick dar. Anschließend wird die Abbildung erläutert und die Erfüllung der Sicherheitsziele durch die Anforderungen begründet.

Tabelle 6.35: Abbildung der Sicherheitsziele für den EVG auf funktionalen Sicherheitsanforderungen

SFR an den EVG	**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**	**O.NK.FW**	**O.NK.Admin_Auth**
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						
FAU_GEN.1/NK.SecLog				X										
FAU_GEN.2/NK.SecLog				X										
FMT_SMR.1/NK			X							X	X			
FMT_MTD.1/NK			X											
FIA_UID.1/NK.SMR			X											
FIA_UAU.1/NK														X
FTP_TRP.1/NK.Admin			X											
FMT_SMF.1/NK			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.FWAuth													**X**	
FDP_ACC.1/NK.FWUpdate													**X**	
FDP_ACF.1/NK.FWUpdate													**X**	
FDP_ITC.1/NK.FWUpdate													**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**					
FIA_UAU.5/NK														**X**

Die Begründung erfolgt für jedes Sicherheitsziel für den EVG in einem eigenen Unterabschnitt.

6.4.1.1 Erfüllung des Zieles O.NK.Schutz

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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.

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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.Schutz und 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.phys_Schutz formulierten Einschränkungen). Der EVG führt beim Start-up und bei Bedarf Selbsttests durch.“ Das Erkennen bzw. Erkennbarmachen sicherheitstechnischer Veränderungen erfolgt durch den von FPT_TST.1/NK geforderten Selbsttest. Im Rahmen der Integritätsprüfungen werden Hashwerte wie von FCS_COP.1/NK.Hash gefordert verwendet. Dieses SFR hat die formalen Abhängigkeiten FCS_CKM.4/NK und FCS_CKM.1/NK, wobei FCS_CKM.4/NK nicht erfüllt werden muss, sofern im Rahmen der Hashwertberechnung keine geheimen Schlüssel verwendet werden. FCS_CKM.1/NK fordert, dass das Schlüsselmaterial (z. B. Integritätsprüfschlüssel) generiert wird.

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Schutz gegen unbefugte Kenntnisnahme (Side Channel-Analysen)	FPT_EMS.1/NK, Verfeinerung zu ADV_ARC.1

Begründung: „Der EVG schützt die von ihm in einem sicheren Schlüsselspeicher gespeicherten Geheimnisse gegen ... jegliche andere unbefugte Kenntnisnahme.“ Um den Aspekt „andere unbefugte Kenntnisnahmen“ vollständig abzudecken, wurde die Komponente FPT_EMS.1/NK analysiert, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen. Die Beschreibung der Sicherheitsarchitektur ist wesentlich für die Beurteilung des Selbstschutzes und der Möglichkeiten, Sicherheitsfunktionen zu umgehen (bypassing).

6.4.1.2 Erfüllung des Zieles O.NK.EVG_Authenticity

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Auslieferungsverfahren: Nur authentische EVGs können in Umlauf gebracht werden	FCS_COP.1/NK.Auth, FCS_CKM.1/NK, FCS_CKM.4/NK, Verfeinerungen zu ALC_DEL.1 und AGD_OPE.1

Begründung: „Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können.“ Das Refinement zu ALC_DEL.1 fordert ein sicheres Auslieferungsverfahren, das Refinement zu AGD_OPE.1 fordert sichere Verfahren zur Inbetriebnahme (zu den Refinements siehe Abschnitt 6.3). „Gefälschte EVGs müssen vom VPN-Konzentrator sicher erkannt werden können. Der EVG muss auf Anforderung mit Unterstützung der SM NK einen Nachweis seiner Authentizität ermöglichen.“ Die Authentisierung wird mit Kryptoalgorithmen erbracht, die durch FCS_COP.1/NK.Auth spezifiziert werden. FCS_CKM.1/NK fordert eine Generierung des für den Nachweis der Authentizität des EVGs erforderlichen Schlüsselmaterials; FCS_CKM.4/NK unterstützt als abhängige Komponenten dabei.

6.4.1.3 Erfüllung des Zieles O.NK.Admin_EVG

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen Identifikation und Authentisierung / Autorisierung des Administrators sicherer Pfad Beschränkung der Administration Hinweise zur Administration	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, Verfeinerung zu AGD_OPE.1

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. FMT_MSA.4/NK weist einem Administrator die Attribute (autorisiert, nicht autorisiert) zu.

„Die Administration erfolgt rollenbasiert.“ FMT_SMR.1/NK modelliert die Rolle Administrator. „Weil die Administration über die lokale Netzverbindung PS1 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.

6.4.1.4 Erfüllung des Zieles O.NK.Admin_Auth

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Authentisierung des Administrators	FIA_UAU.1/NK FIA_UAU.5/NK

Begründung: Die Authentisierung des Administrators findet statt, bevor eine administrative Operation ausgeführt wird. Dies wird von FIA_UAU.1/NK gefordert.

Der EVG setzt die Authentisierung des Administrators vor der Ausführung administrativer Operationen durch. Mittels FIA_UAU.5/NK werden die Regeln zur Authentisierung und Autorisierung eines Administrators aus dem Netz des Leistungserbringers und aus dem Netz des sicheren Internet-Service modelliert.

6.4.1.5 Erfüllung des Zieles O.NK.Protokoll

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
EVG protokolliert sicherheitsrelevante Ereignisse mit Daten und Zeitstempel	FAU_GEN.1/NK.SecLog, FAU_GEN.2/NK.SecLog, FPT_STM.1/NK

Begründung: „Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit." → FAU_GEN.1/NK.SecLog fordert eine Protokollierung für die in der Operation explizit aufgelisteten Ereignisse und stellt Anforderungen an den Inhalt der einzelnen Log-Einträge. FAU_GEN.2/NK.SecLog fordert, dass die Benutzeridentitäten mit protokolliert werden. FPT_STM.1/NK stellt den Zeitstempel bereit.

6.4.1.6 Erfüllung des Zieles O.NK.Zeitdienst

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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.

6.4.1.7 Erfüllung des Zieles O.NK.VPN_Auth

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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_TI (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 ein gSMC-K, welches in den EVG eingebracht wird). FCS_CKM.4/NK unterstützt als abhängige Komponente.

6.4.1.8 Erfüllung des Zieles O.NK.Zert_Prüf

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Gültigkeitsprüfung von Zertifikaten mit Hilfe von TSL, dem OCSP Dienst und der CRL	FPT_TDC.1/NK.Zert

Begründung: Zertifikatsprüfung: „Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form der TSL sowie eines OCSP-Dienstes und einer zugehörigen CRL 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 bzw. OCSP explizit erwähnt: „The TSF shall provide the capability to consistently interpret information – distributed in the form of a TSL (Trust-Service Status List) with CRL (Certificate Revocation List) information and by an OCSP responder ...“ 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.

6.4.1.9 Erfüllung des Zieles O.NK.VPN_Vertraul

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Vertraulichkeit der Nutzdaten im VPN (Telematikinfrastruktur-Netz) IPsec-Kanal: Ableitung von session keys, AES-Verschlüsselung mit den session keys , Zerstörung der session keys nach Verwendung, Geheimhaltung der session keys	FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS, FCS_COP.1/NK.IPsec, → FCS_CKM.1/NK, → FCS_CKM.2/NK.IKE, → FCS_COP.1/NK.ESP, → FCS_CKM.4/NK, FPT_EMS.1/NK

Begründung: „Der EVG schützt die Vertraulichkeit der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren verschlüsselt (vor dem Versand) bzw. entschlüsselt (nach dem Empfang) der Konnektor die Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Verschlüsselung wird durch FTP_ITC.1/NK.VPN_TI (im Fall der Telematikinfrastruktur) bzw. FTP_ITC.1/NK.VPN_SIS (im Fall des Sicheren Internet Service) gefordert („. . . protection of the channel data from modification and disclosure“, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.IPsec ermöglicht die Definition der zu verwendenden Verschlüsselungsalgorithmen, hier AES gemäß FCS_COP.1/NK.ESP. FCS_CKM.4/NK unterstützt als abhängige Komponente ebenfalls. Für einzelne Verbindungen werden jeweils eigene session keys aus dem langfristig gültigen Schlüsselmaterial im X.509-Zertifikat 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.

6.4.1.10 Erfüllung des Zieles O.NK.VPN_Integrität

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von session keys, Austausch der session keys mit Gegenstelle, Zerstörung der session keys nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von session keys, Zerstörung der session keys nach Verwendung Geheimhaltung der session keys	FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS, FCS_COP.1/NK.Hash, FCS_CKM.1/NK, FCS_CKM.2/NK.IKE, FCS_CKM.4/NK, FCS_COP.1/NK.HMAC, FCS_CKM.1/NK, FCS_CKM.4/NK, FPT_EMS.1/NK

Begründung: „Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Integritätssicherung wird durch FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS gefordert („. . . protection of the channel data from modification and disclosure“, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Authentication Header (RFC 4302 (AH), [32]) erfolgt, wobei die Authentizitätsdaten (authentication data) den Wert des Integritätstests (integrity check value) enthalten, der sich wiederum aus einem Hash des übrigen Paketes ergibt. Insofern ist eine Hashfunktion erforderlich. Weiterhin ist im IPSec sowie in IKE Standard die Verwendung von HMAC Algorithmen enthalten ([40], [41], [35]). Dies wird durch FCS_COP.1/NK.HMAC erreicht. Für einzelne Verbindungen werden jeweils eigene session keys aus dem langfristig gültigen Schlüsselmaterial im X.509-Zertifikat 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.

6.4.1.11 Erfüllung des Zieles O.NK.PF_WAN

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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 Client-Systeme vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN).“ → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects VPN concentrator and attacker communicating with the TOE from its WAN interface (PS3) . . . “ FDP_IFF.1/NK.PF modelliert einen Paketfilter („. . . the decision shall be based on the following security attributes: IP address, port number, and protocol type.“, „For every operation (. . .) the TOE shall maintain a set of packet filtering rules . . . “). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (Stateful Packet Inspection) abgebildet und durch ein Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF (für die Paketfilterregeln im Allgemeinen). Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen (z. B Administrator) und verhindert so unbefugte Veränderungen an den sicherheitsrelevanten Filterregeln. FMT_SMR.1/NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf. „Es werden Angreifer mit hohem Angriffspotential betrachtet.“ → Das Angriffspotential wird durch AVA_VAN.5 bestimmt (AVA_VAN.5 fordert Resistenz gegen Angreifer mit hohem Angriffspotential).

6.4.1.12 Erfüllung des Zieles O.NK.PF_LAN

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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, AVA_VAN.5 (hohes Angriffspotential), 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: Client-System) communicating with the TOE from its LAN interface (PS2) ...“ FDP_IFF.1/NK.PF modelliert einen Paketfilter („... the decision shall be based on the following security attributes: IP address, port number, and protocol type.“, „For every operation (...) the TOE shall maintain a set of packet filtering rules ...“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (Stateful Packet Inspection) abgebildet und durch das folgende Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen. FMT_SMR.1/NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf. „Es werden Angreifer mit hohem Angriffspotential betrachtet.“ → Das Angriffspotential wird durch AVA_VAN.5 bestimmt (AVA_VAN.5 fordert Resistenz gegen Angreifer mit hohem Angriffspotential). „Für zu schützende Daten der TI erzwingt der EVG die Nutzung des VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Client-Systemen) 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 6.3.2.

6.4.1.13 Erfüllung des Zieles O.NK.Stateful

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
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.

6.4.1.14 Erfüllung des Zieles O.NK.FW

Aspekt des Zieles	**Erfüllung durch SAR, SFR**
Authentizitätsprüfung von Firmware-Updates und Durchsetzung des Firmware-Gruppenkonzepts	FCS_COP.1/NK.FWAuth, FDP_ACC.1/NK.FWUpdate, FDP_ACF.1/NK.FWUpdate, FDP_ITC.1/NK.FWUpdate

Begründung: „Der EVG installiert nur geprüfte und als authentisch festgestellte Daten als Firmware-Update.“ Daten sind als authentisches Firmware-Update anzusehen, wenn sie vom Herausgeber als Firmware-Update digital signiert wurden. Der EVG stellt dies fest, indem er eine Signaturprüfung der heruntergelednen Daten vornimmt. Dies wird durch FCS_COP.1/NK.FWAuth modelliert. Die Erfüllung der Abhängigkeit FCS_CKM.4 ist nicht erforderlich, da der öffentliche Schlüssel auf dem Sicherheitsmodul gespeichert ist und die Kenntnis dieses Schlüssels durch einen Angreifer keine neuen Bedrohungen nach sich zieht. Die Durchsetzung der Prüfung und die Einhaltung der Vorgaben an das Firmware-Gruppenkonzept gemäß [57], Abschnitt 2.5 wird mithilfe von FDP_ACC.1/NK.FWUpdate, FDP_ACF.1/NK.FWUpdate, FDP_ITC.1/NK.FWUpdate abgebildet.

6.4.2 Erfüllung der Abhängigkeiten

6.4.2.1 Erfüllung der funktionalen Anforderungen

In Abschnitt 6.2 wird für jede funktionale Anforderung die Menge aller von ihr abhängigen Komponenten unter dem Stichwort **Dependencies** aufgeführt. Die Erfüllung der Abhängigkeiten wird jeweils nach der Angabe **hier erfüllt durch** demonstriert. Wird eine Abhängigkeit nicht erfüllt, so wird dies angezeigt durch den Satz **Diese Abhängigkeit wird nicht erfüllt.** nach dem Stichwort **Begründung** wird 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 ist in sich konsistent und erfüllt alle Abhängigkeiten. Die Abhängigkeiten der im Rahmen der Augmentierung neu hinzugekommenen Komponenten (siehe Abschnitt 1.1) werden ebenfalls erfüllt, wie die folgende Tabelle 6.36 zeigt.

Augmentierung	**Abhängigkeit(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 6.36: Erfüllung der Abhängigkeiten der augmentierten Komponenten

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 Kapitel 5 definiert. Diese erweiterte Komponente wurde bereits im PP COS G2 [13], 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 das gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG soll darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll verhindern, etwa die mit Hilfe des gSMC-K abgeleiteten Session Keys. Ein Beispiel für solche Angriffe sind Timing-Angriffe. 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).

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, da diese Stufe auch in der Anlage 1

der Signaturverordnung [11] gefordert wird und nur bei gleichen Anforderungen an die Vertrauenswürdigkeit übergreifende Sicherheitsfunktionalität zwischen dem PP Konnektor ORS1 und dem NK-PP flexibel zugeordnet werden kann.

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.

Kapitel 7

Zusammenfassende Spezifikation der Sicherheitsfunktionalität

Die zusammenfassende Spezifikation der Sicherheitsfunktionalität des Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 erklärt, wie die einzelnen funktionale Sicherheitsanforderungen aus Abschnitt 6.2 durch die vom EVG bereitgestellten Sicherheitsfunktionen erfüllt werden. Der Abstraktionsgrad ist dabei so gewählt, dass dem Leser ein allgemeiner Eindruck vermittelt wird, ohne dabei jedoch auf Einzelheiten der Implementierung einzugehen.

Tabelle 7.1: Abbildung der Sicherheitsfunktionalität auf funktionale Sicherheitsanforderungen

SFR / SF	**SF1: VPN-Client**	**SF2: Dynamischer Paketfilter**	**SF3: Netzdienste**	**SF4: Selbstschutz**	**SF5: Administration**	**SF6: Kryptographische Basisdienste**	**SF7: Firmware-Update**
FTP_ITC.1/NK.VPN_TI	X						
FTP_ITC.1/NK.VPN_SIS	X						
FDP_IFC.1/NK.PF		X					
FDP_IFF.1/NK.PF		X					
FMT_MSA.3/NK.PF		X					
FPT_STM.1/NK			X				
FPT_TDC.1/NK.Zert	X						
FDP_RIP.1/NK				X			
FPT_TST.1/NK				X			
FPT_EMS.1/NK				X			
FAU_GEN.1/NK.SecLog				X			

FAU_GEN.2/NK.SecLog				**X**			
FMT_SMR.1/NK					**X**		
FMT_MTD.1/NK					**X**		
FIA_UID.1/NK.SMR					**X**		
FIA_UAU.1/NK					**X**		
FTP_TRP.1/NK.Admin				**X**	**X**		
FMT_SMF.1/NK					**X**		
FMT_MSA.1/NK.PF					**X**		
FMT_MSA.4/NK					**X**		
FCS_COP.1/NK.Hash						**X**	
FCS_COP.1/NK.HMAC						**X**	
FCS_COP.1/NK.Auth						**X**	
FCS_COP.1/NK.FWAuth						**X**	**X**
FDP_ACC.1/NK.FWUpdate							**X**
FDP_ACF.1/NK.FWUpdate							**X**
FDP_ITC.1/NK.FWUpdate							**X**
FCS_COP.1/NK.ESP						**X**	
FCS_COP.1/NK.IPsec						**X**	
FCS_CKM.1/NK						**X**	
FCS_CKM.2/NK.IKE						**X**	
FCS_CKM.4/NK						**X**	
FIA_UAU.5/NK					**X**		

7.1 SF1: VPN-Client

Die vom VPN-Client des Netzkonnektors zu erfüllenden funktionalen Sicherheitsanforderungen sind im Abschnitt 6.2.1 abschließend angegeben.

Der EVG stellt sichere Kommunikationskanäle zur Telematik-Plattform und zum sicheren Internet-Service (SIS) bereit. Diese Kommunikationskanäle werden vom Netz- und Anwendungskonnektor als auch von Client-Systemen genutzt, um mit Diensten hinter diesen Endpunkten zu kommunizieren. Die Kommunikationskanäle werden durch den EVG aufgebaut und verwaltet. Dazu muss die interne Zustandsvariable des Netzkonnektors *MGM_LU_ONLINE* gesetzt sein, deren Semantik darin besteht, dass der Konnektor eine Verbindung zum Weitverkehrsnetz (WAN) herstellt und in Folge dessen die sicheren Kommunikationskanäle aufbaut. Die Verbindung zum sicheren Internet-Service wird nur dann hergestellt, wenn der Konnektor zur Nutzung des sicheren Internet-Service konfiguriert ist. Der Aufbau der Verbindung erfolgt automatisch nach dem Start des Konnektors und kann vom Administrator des Konnektors abgebaut und erneut aufgebaut werden.

Die Ermittlung der IP-Adressen der VPN-Endpunkte zur Telematik-Plattform als auch zum sicheren Internet-Service werden unter Verwendung des Protokolls DNSSEC ermittelt. Der empfangene DNS-Record muss authentisch und in der Kette gegen den IANA-Vertrauensanker prüfbar sein. Die zur Prüfung der X.509-Zertifikate der Endpunkte erforderliche(n) Sperrliste(n) werden vom Konnektor vor dem Verbindungsaufbau aus dem Internet heruntergeladen.

Der sichere Kommunikationskanal wird unter Verwendung des Protokolls IPSec geschützt, der Aufbau der Verbindung erfolgt unter Verwendung des Protokolls IKEv2. Im Zuge des Verbindungsaufbaus authentisiert sich der Konnektor gegenüber den Endpunkten und authentisiert diese ebenfalls. Die Authentisierung des Konnektors erfolgt unter Verwendung der auf der gSMC-K befindlichen Netzkonnektoridentität ID.NK.AUTH und deren zugeordneten privaten Schlüssel und dem zugehörigen X.509-Zertifikat. Die Authentisierung der Endpunkte erfolgt gemäß den Vorgaben der Konnektorspezifikation. Die von den Endpunkten präsentierten Zertifikate müssen:

a) strukturell den Anforderungen der [18] entsprechen

b) die korrekten Attribute für ein Konzentratorzertifikat gemäß Gematik OID- und PKI-Spezifikation ([21] und [22]) aufweisen

c) die vom Konnektor akzeptierten kryptografischen Algorithmen verwenden[1]

d) zum Zeitpunkt des Verbindungsaufbaus gemäß Prüfung der Ausstellungs- und Ablaufdaten gültig sein

e) zum Zeitpunkt des Verbindungsaufbaus gemäß Prüfung gegen eine Sperrliste gültig sein

f) aus der zugeordneten CA abgeleitet sein, die ihrerseits in der Trusted Service List der Gematik geführt wird

Das IKEv2-Verfahren unterscheidet zwischen der Möglichkeit, dass die Zertifikate der Endpunkte als Teil der Nachricht *SA_AUTH* oder mit Hilfe des Verfahrens Hash&URL übertragen werden. Beide Varianten werden vom Netzkonnektor unterstützt, wobei die Nutzung des Verfahrens Hash&URL explizit durch den Administrator vorgegeben werden muss.

In der Phase der Aushandlung der *Security Association* werden die kryptografischen Parameter ausgehandelt, die anschließend von den IPSec gesicherten Kanälen verwendet werden. Diese Kanäle logisch voneinander getrennt, dabei beide Kanäle verschiedenen Endpunkten mit verschiedenen Identitäten zugeordnet sind[2] und durch die Verwendung des IKEv2-Protokolls verschiedene kryptografische Schlüssel (so auch den symmetrischen AES-256 Schlüssel) innehaben. Beide Kanäle verfügen über unterschiedliche innere Tunnel-IP Adressen.

[1] Siehe hierzu Verfeinerung zu FPT_ITC.1/NK.Zert, der EVG muss prüfen ob die Algorithmen gemaß technischer Richtlinie TR-03116 noch gültig sind.

[2] Die Endpunkte für die Telematik-Plattform und den sicheren Internet-Service werden mittels ihrer X.509-Zertifikate authentisiert

Mit Hilfe des IPSec-Protokolls werden die Anforderungen an die Authentizität und die Vertraulichkeit der übertragenen Daten umgesetzt. Durch das Vorgehen des EVG werden die Sicherheitsanforderungen **FTP_ITC.1/NK.VPN_TI** und **FTP_ITC.1/NK.VPN_SIS** umgesetzt. Mit der Funktionalität der Zertifikatsprüfung wird die Anforderung **FPT_TDC.1/NK.Zert** umgesetzt.

7.2 SF2: Dynamischer Paketfilter

Die vom dynamischen Paketfilter des Netzkonnektors zu erfüllenden funktionalen Sicherheitsanforderungen sind im Abschnitt 6.2.2 abschließend angegeben.

Der EVG beinhaltet die Funktionalität eines dynamischen Paketfilters. Diese Funktionalität wird an der LAN und an der WAN-Schnittstelle durchgesetzt und adressiert mithin die in **FDP_IFC.1.1/NK.PF** angegebenen Subjekte, Informationen und Operationen. Dem EVG sind die in **FDP_IFC.1.1/NK.PF** aufgeführten Adressen und Adressbereiche explizit bekannt. Diese Informationen werden vom EVG zur Aufstellung von Routing-Einträgen und zur korrekten Anwendung der Firewallregeln genutzt. Der EVG setzt eine default-deny Strategie um (**FDP_IFF.1.5/NK.PF**). Dies bedeutet, dass sämtlicher Datenverkehr außer dem explizit Zugelassenen unterbunden wird. In die Entscheidung über zulässigen Datenverkehr fließen zudem die Informationen

I) IP-Adresse

II) Port

III) Protokoll Typ

IV) Richtung (Ein- und Ausgehend)

zur Umsetzung der Anforderung **FDP_IFF.1/NK.PF** ein. Der EVG erlaubt hingegen explizit den Datenfluss gemäß den in **FDP_IFF.1.2/NK.PF** aufgestellten Regeln. Mit Hilfe dieser definierten Regeln schützt der EVG das Netz des Leistungserbringers gegen Angriffe aus dem WAN und unterbindet den Datenverkehr aus dem Netz des Leistungserbringers in das WAN außer zum Zwecke des Verbindungsaufbaus zu den VPN-Konzentratoren der Telematik-Plattform oder des sicheren Internet-Service. In diese Regeln fließen die Informationen zu IP-Adressen und Netzsegmenten gemäß **FDP_IFC.1.1/NK.PF** ein. Diese Firewallregeln sind restriktiv und werden vom Konnektor als default-Regeln auf den Datenverkehr angewandt, womit der EVG **FMT_MSA.3/NK.PF** umsetzt. Pakete, zu denen keine Regel existiert[3], werden verworfen.

Die Datenübertragung ins WAN wird nur dann gestattet, wenn ein IPSec-Tunnel aufgebaut wurde und dieser Tunnel aktiv ist[4]. Damit setzt der EVG die Anforderung **FDP_IFF.1.3/NK.PF** und **FDP_IFF.1.4/NK.PF** durch.

[3]Das ist gleichbedeutend mit der Feststellung, dass das Paket nicht weitergeleitet werden darf.

[4]Darunter ist zu verstehen, dass der Datenverkehr ins WAN, beispielsweise im Zuge der Kommunikation mit dem VSDM-Fachdienst nur dann ermöglicht wird, wenn der zugehörige VPN-Tunnel besteht.

In der Durchsetzung der Firewallregeln besteht eine Abhängigkeit zum Konfigurationswert *MGM_LU-_ONLINE*. Ist dieser Wert auf *falsch* eingestellt, soll keine Kommunikation mit dem WAN möglich sein. Aus diesem Grunde wird vom EVG bei *MGM_LU_ONLINE = falsch* der WAN-Adapter deaktiviert. In diesem Falle werden auf Grund der Deaktivierung der physischen Schnittstelle keine weiteren Firewallregeln angewandt, da der Datenfluss komplett unterbunden wird[5].

Eine weitere Abhängigkeit besteht zum Konfigurationswert *MGM_LOGICAL_SEPARATION*. Ist der Wert dieses Konfigurationswertes auf *wahr* gestellt, werden keine Datenpakete aus dem Netz des Leistungserbringers in Netze geleitet, die über die WAN-Schnittstelle erreichbar sind.

7.3 SF3: Netzdienste

Die von den Netzdiensten des Netzkonnektors zu erfüllenden funktionalen Sicherheitsanforderungen sind im Abschnitt 6.2.3 abschließend angegeben.

Der EVG stellt einen NTP-Server der Stratum-3-Ebene für Fachmodule und Client-Systeme bereit, welcher die Zeitangaben eines NTP Servers Stratum-2-Ebene der zentralen Telematikinfrastruktur-Plattform in regelmäßigen Abständen abfragt[6]. In Übereinstimmung mit Abschnitt 7.1 erfolgt die Abfrage in einem sicheren Kanal. Abgefragte Zeit und interne Zeit des Netzkonnektors werden miteinander abgeglichen. Die zulässige Abweichung beträgt 330 Millisekunden. Nicht korrigierbare Abweichungen von mehr als 330 Millisekunden werden der Einsatzumgebung durch eine LED- und 7-Segment Anzeige (nur LS-Konnektor) und dem Anwendungskonnektor mit Hilfe einer internen Ereignismeldung signalisiert. Dadurch wird die Anforderung **FPT_STM.1/NK** erfüllt.

Der EVG stellt die synchronisierte Zeit anderen Komponenten des Konnektors auf Anfrage zur Verfügung. Die vom EVG bereitgestellte Zeit-Information wird unter anderem genutzt, um die Audit-Daten des Sicherheits-Logs mit einer Zeitangabe zu versehen.

Der EVG stellt Fachmodulen und Client-Systemen weitere Netzdienste bereit, die nachfolgend aufgeführt werden.

1. DHCP-Server Funktionalität auf der Netzseite des Leistungserbringers
2. Caching DNS-Resolver Funktionalität auf der Netzseite des Leistungserbringers mit der Möglichkeit zur Auflösung eines DNS-Request im WAN

Mit Hilfe des DHCP-Servers des Netzkonnektors können Client-Systemen dynamisch eine IP-Adresse in dem vorgegebenen Netzsegment beziehen. Mit Hilfe des Caching DNS-Resolvers können Client-Systeme eine DNS-Anfrage stellen und diese in den verschiedenen, vom Konnektor erreichbaren

[5] Gilt bei Betrieb in Reihe. Bei parallelem Betrieb ist der WAN-Adapter ohnehin deaktiviert, der Netzverkehr erfolgt in diesem Falle komplett über die LAN-Schnittstelle. In diesem Falle wird die Kommunikation in Richtung LAN an der betreffenden physischen Schnittstelle komplett blockiert.

[6] Gemäß FPT_STM.1/NK erfolgt die Abfrage der Zeit aus dem Kanal zur Telematik-Plattform alle 24 Stunden.

Netzsegmenten auflösen lassen. Diese Möglichkeit wird ebenfalls durch die Konfigurationsvariablen *MGM_LU_ONLINE* und *MGM_LOGICAL_SEPARATION* beeinflusst. Ist *MGM_LU_ONLINE* = *falsch*, kann der DNS-Resolver keine Anfragen in Netzsegmenten auflösen, die im WAN erreichbar sind. Ist *MGM_LOGICAL_SEPARATION* = *wahr*, leitet der DNS-Resolver keine Anfragen aus dem Netz des Leistungserbringers in Netze weiter, die über das Weitverkehrsnetz erreichbar sind.

7.4 SF4: Selbstschutz

Die für den Selbstschutz des Netzkonnektors zu erfüllenden funktionalen Sicherheitsanforderungen sind im Abschnitt 6.2.5 abschließend angegeben.

Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben.[7] Der EVG löscht ferner durch aktives Überschreiben und ein randomisiertes Speicherlayout alle empfangenen *zu schützende Daten der TI und der Bestandsnetze* und *zu schützenden Nutzdaten*, und zwar entweder unmittelbar nach dem Versand oder unmittelbar nach dem Verwerfen. Dadurch wird die Anforderung **FDP_RIP.1/NK** erfüllt.

Beim Start-up führt der EVG alle erforderlichen Tests durch, um seine eigene Integrität festzustellen. Im Fall einer Integritätsverletzung zeigt der EVG dies an[8]. Zusätzlich bietet der EVG seinen autorisierten Benutzern eine Möglichkeit, die Integrität des EVGs und seiner TSF-Daten zu prüfen, und macht dadurch sicherheitstechnische Veränderungen am EVG für den Anwender erkennbar[9]. Im Einzelnen werden jeweils folgende Prüfungen durchgeführt:

- die Prüfung kryptographischer Verfahren bei Programmstart[10],
- die Prüfung des statischen Kernels (Signaturprüfung),
- die Prüfung des Dateisystems des EVGes und
- die Prüfung der Signaturen vorhandener (vom Hersteller angepasster) SW-Komponenten im Netzkonnektor.

[7] Diese Löschfunktion bezieht sich nur auf solche Schlüssel, die im EVG selbst abgelegt oder vom EVG selbst benutzt werden. Im Sicherheitsmodul gSMC-K abgelegte und nur vom gSMC-K selbst benutzte Schlüssel sind von dieser Funktionalität (natürlich) nicht betroffen.

[8] Damit der EVG eine Integritätsverletzung anzeigen kann, muss die Phase der sicheren Initialisierung durchlaufen worden sein. Eine Integritätsverletzung wird dem authentisierten Administrator mit Hilfe des Sicherheits-Protokolls zur Kenntnis gebracht. Zudem signalisiert der EVG eine Integratitätsverletzung durch die Signaleinrichtung (LED und 7-Segment Anzeige)

[9] Diese Möglichkeit besteht für den autorisierten Administrator durch die Möglichkeit, einen Neustart herbei zu führen.

[10] Dies betrifft insbesondere vom EVG genutzte AES- und Hash-Implementierungen

Auf diese Weise wird die Anforderungen **FPT_TST.1/NK** erfüllt.

An der LAN-Schnittstelle PS2 und an der WAN-Schnittstelle PS3 werden im Wesentlichen verschlüsselte Signale abgestrahlt. Ob aus den verschlüsselten Signalen Rückschlüsse auf die benutzten Schlüssel gezogen werden können, hängt daher lediglich von der Stärke der eingesetzten Verschlüsselung ab. Da hierbei die Festlegungen aus [14] beachtet werden, sind die Algorithmen hinreichend stark und lassen keinen Rückschluss auf das verwendete Schlüsselmaterial zu. Die an PS3 ansonsten abgestrahlten, unverschlüsselten Signale sind Protokolldaten, die dem Aufbau eines sicheren Kanals dienen. Das benutzte IPsec-Protokoll ist sicher in dem Sinne, dass aus den Daten, die dem Kanalaufbau dienen, keine Rückschlüsse auf das verwendete (oder zu verwendende) Schlüsselmaterial gezogen werden können.

Schlüsselmaterial, das zur Feststellung der Integrität und Herkunft von Updates benutzt wird, ist von der Übertragung über PS2 oder PS3 ausgeschlossen. Die Anmeldung eines Administrators ist so gestaltet, dass zunächst ein sicherer Kanal aufgebaut wird(**FTP_TRP.1/NK.Admin**). Weitere Daten zur Identifizierung und Authentisierung von Administratoren werden anschließend im gesicherten Kanal übertragen, der keine Rückschlüsse auf die ggf. übertragenen Geheimnisse zuläßt.

Zudem verfügt der EVG über keine Funktionalität, die eine direkte Abfrage von Schlüsselmaterial oder anderen Geheimnissen ermöglichen würde. Daher wird die Anforderung **FPT_EMS.1/NK** erfüllt.

Der EVG führt ein Sicherheits-Log (security log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher ist hinreichend groß dimensioniert. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [16]. Die Auswertung des Sicherheits-Logs erfolgt in der Einsatzumgebung. Für jedes zu protokollierende Ereignis werden (mindestens) folgende Daten aufgezeichnet:

- der Zeitpunkt, zu dem das Ereignis protokolliert wird (d. s. Datum und Uhrzeit),
- die Art des Ereignisses,
- eine Angabe zum Verursacher,
- eine Statusinformation, z. B. Erfolg oder Misserfolg einer protokollierten Aktion

Die Anforderungen **FAU_GEN.1/NK.SecLog** und **FAU_GEN.2/NK.SecLog** werden also erfüllt.

7.5 SF5: Administration

Der EVG unterscheidet im Sinne von **FMT_SMR.1/NK** drei Arten von Subjekten: Administratoren und die VPN-Endpunkte zur Telematik-Plattform und zum sicheren Internet-Service. Die Unterscheidung zwischen den VPN-Endpunkten erfolgt auf Basis der jeweiligen Zertifikate, die Unterscheidung

der Administratoren erfolgt unter Verwendung der Kombination aus Nutzername und Passwort[11]. Demnach ist die Anforderung **FMT_SMR.1/NK** erfüllt.

Der Konnektor unterstützt folgende Typen von Administratoren:

1. Den LAN-seitigen Administrator[12]
2. Den LAN-seitigen Super-Administrator[13]

Hinweis: Der EVG unterstützt keine entfernte Administration.

Der EVG bietet eine Managementschnittstelle an und erzwingt die Authentisierung des Administrators mit Zuweisung eines Sicherheitsattributs zur aktiven Sitzung (**FMT_MSA.4/NK**), bevor dieser administrative Operationen ausführen kann (**FIA_UAU.1/NK**). Der Konnektor authentisiert sich gegenüber dem lokalen Administrator unter Verwendung der Identität ID.AK.AUT mit dem zugehörigen Schlüsselpaar und Zertifikat. Auf der Seite des Leistungserbringers authentisiert sich der Administrator gegenüber dem Netzkonnektor innerhalb des sicheren Kanals mit Nutzername und Passwort (**FIA_UAU.5/NK**).

Während der erstmaligen Anmeldung des Administrators am Konnektor wird dieser aufgefordert, das ursprünglich vergebene Passwort zu ändern. Dabei ist es nicht möglich, das zuvor bereits verwendete Passwort erneut zu benutzen. Die Anforderungen an ein Passwort entsprechend dabei den Vorgaben der Konnektorspezifikation (vgl. [16]).

Der Administrator muss ein Passwort wählen, welches den folgenden Anforderungen entspricht:

- Die Zeichen eines Passworts müssen aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern gewählt werden. Ein Passwort muss Zeichen aus mindestens drei dieser Zeichenklassen enthalten.
- ein Passwort muss mindestens 8 Zeichen lang sein
- ein Passwort darf nicht die zugehörige Benutzerkennung enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung)

Die Wiederholung alter Passwörter beim Passwortwechsel durch den Benutzer selbst wird vom Konnektor verhindert. Dazu erkennt der Konnektor mindestens die letzten drei Passwörter eines Benutzers bei der Passwortneuvergabe und lehnt diese als neues Passwort ab.

Authentisierte Administratoren können die Systemzeit verändern und bestimmte Filterregeln setzen (**FMT_MSA.1/NK.PF**). Diese Funktion steht nur solchen Administratoren zur Verfügung

[12]Zugriff ausschließlich aus dem Netz des Leistungserbringers
[13]Zugriff ausschließlich aus dem Netz des Leistungserbringers

und setzt demnach **FMT_MTD.1/NK** und **FMT_SMF.1/NK** durch. Administrative Tätigkeiten können nur von identifizierten und authentisierten Administratoren ausgeführt werden (**FIA_UID.1/NK.SMR**).

Die Managementfunktion zur Änderung von Filterregeln ist beschränkt auf solche Regeln, die nicht zu einem unsicheren Zustand führen können. Dazu sind gewisse Filterregeln ausgezeichnet, die nicht im Rahmen normaler Administratortätigkeit verändert oder gelöscht werden können. Für den Fall, dass eine Änderung solcher gekennzeichneter Filterregeln erforderlich werden sollte, sieht der EVG den Weg über die Benutzung eines (autorisierten) Updates vor.

7.6 SF6: Kryptographische Basisdienste

Der EVG stellt alle benötigten kryptographischen Basisdienste zur Verfügung. Im Einzelnen sind dies folgende Dienste:

(a) **Hashfunktionen:** SHA-1, SHA-256, SHA-384, SHA-512 für die SFR **FCS_COP.1/NK.Hash** und **FCS_COP.1/NK.HMAC**

(b) **Signaturfunktionen:** SHA-256 mit RSA-Verschlüsselung, Schlüssellänge 2048 Bits für die SFR **FCS_COP.1/NK.Auth**

(c) **Symmetrische Ver- und Entschlüsselung:** AES (mit 256 Bit Schlüssellänge) im CBC-Mode für **FCS_COP.1/NK.ESP**

(d) **Protokolle:** IPsec, IPsec IKE v2 für **FCS_COP.1/NK.IPsec**, **FCS_CKM.2/NK.IKE**

(e) **Schlüsselgenerierung:** Die Generierung (temporärer) Schlüssel erfolgt unter Benutzung des Sicherheitsmoduls gSMC-K, wodurch **FCS_CKM.1/NK** erfüllt wird.

(f) **Schlüsselvernichtung:** Nicht mehr benötigte Schlüssel und andere Geheimnisse werden durch Überschreiben mit einem festen Wert gelöscht, vgl. **FCS_CKM.4/NK**.

(g) **Firmware-Updates** werden mithilfe der funktionalen Sicherheitsanforderung **FCS_COP.1/NK.FWAuth** hinsichtlich ihrer Integrität und Authentizität geprüft. Die Prüfung erfolgt an Signaturen mit SHA-256 Hashwerten und einer Schlüssellänge von 2048 und 4096 Bit

Auf diese Weise werden alle in Abschnitt 6.2.7 aufgeführten Anforderungen erfüllt.

7.7 SF7: Firmware-Update

Der EVG setzt das Firmwaregruppen-Konzept gemäß [57] um und bietet diesen Mechanismus für folgende Zwecke an:

- Aktualisierung des UEFI
- Aktualisierung des verwendeten Betriebssystems
- Aktualisierung der Netzkonnektorsoftware
- Aktualisierung des Anwendungskonnektors (kein EVG-Bestandteil)
- Hinzufügen und Aktualisierung von Fachmodulen (kein EVG-Bestandteil)

Eine Firmwaregruppe ist gemäß [57] eine Gruppe zulässiger Komponentenversionen, die zueinander kompatibel und betriebsfähig sind. Der EVG beinhaltet exakt eine zulässige Version des UEFI, des Betriebssystems und der Netzkonnektorsoftware, so wie in Tabelle 1.1 angegeben. Der EVG setzt die folgenden Anforderungen aus [57] durch.

Tabelle 7.2: Vom EVG umgesetzte Anforderungen aus [57]

Anforderung	**Beschreibung**
GS-A_4866	Integritäts- und Authentizitätsschutz der Firmware-Versionsinformationen
GS-A_4867	Übernahme Firmware-Gruppe
GS-A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe
GS-A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version
GS-A_4872	Kein Downgrade der Firmware-Gruppe
GS-A_4873	Speicherung der Firmware-Gruppe
GS-A_4874	Firmware-Gruppen-Updates nur über herstellereigenen Update-Mechanismus

Der Integritäts- und Authentizitätsschutz gemäß GS-A_4866 wird mithilfe einer elektronischen Signatur umgesetzt, die Prüfung der Signatur erfolgt durch **FCS_COP.1/NK.FWAuth**. Die Vorgaben des Firmware-Gruppenkonzepts gemäß [57], Abschnitt 2.5 werden mithilfe der funktionalen Sicherheitsanforderungen **FDP_ACC.1/NK.FWUpdate**, **FDP_ACF.1/NK.FWUpdate**, **FDP_ITC.1/NK.FWUpdate** abgebildet.

Anhang A

Kryptographische Funktionalitäten

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
1	Authenticity	RSA signature verification with encoding RSASSA-PKCS1-1.5 using SHA-256	RFC 3447 [25] (RSA), FIPS180-4 [26] (SHA)	2048	FPT_TDC.1/ NK.Zert, FCS_COP.1/ NK.Auth, FTP_TRP.1/ NK.Admin
2	Authentication	RSA signature creation with support of gSMC-K and verification with encoding RSASSA-PKCS1-1.5 using SHA-256	RFC 3447 [25] (RSA), FIPS180-4 [26] (SHA)	2048	FCS_COP.1/ NK.Auth, FTP_TRP.1/ NK.Admin
3	Key Agreement	Diffie-Hellman (IKEv2) with key derivation function PRF-HMAC-SHA-1, SHA-256	Handbook of Applied Cryptography [60] (DH), RFC 3526 [42] (DH-group), FIPS180-4 [26] (SHA), RFC 2104 [50] (HMAC), RFC 5996 [36] (IKEv2), RFC 5869 [62]	2048 (dh-group 14) with DH exponent length =384 bits	FCS_CKM.2/ NK.IKE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
4	Key Agreement	Diffie-Hellman with TLS key derivation function	Handbook of Applied Cryptography [60] (DH), RFC 3526 [42] (DH-group), FIPS180-4 [26] (SHA), RFC 1321 [51] (MD5), RFC 2104 [50] (HMAC), RFC 4346 [29] (TLSv1.1) RFC 5246 [30] (TLSv1.2)	2048 (dh-group 14) with DH exponent length =384 bits	FTP_TRP.1/ NK.Admin
5	Key Agreement	EC Diffie-Hellman with TLS key derivation function	RFC 4492 [52] (ECC for TLS), RFC 4346 [29] (TLSv1.1), RFC 5246 [30] (TLSv1.2)	Key sizes corresponding to the used elliptic curves P-{256, 384} FIPS 186-4 [27], brainpoolP{256, 384, 512}r1 (RFC 5639 [53], RFC 7027 [54]	FTP_TRP.1/ NK.Admin
6	Confidentiality	AES in CBC mode	FIPS 197 [28] (AES), RFC 3602 [39] (AES-CBC)	256	FCS_COP.1/ NK.ESP, FCS_COP.1/ NK.IPsec, FCS_CKM.2/ NK.IKE
7	Confidentiality	AES in CBC mode	FIPS 197 [28] (AES), RFC 3602 [39] (AES-CBC)	128, 256	FTP_TRP.1/ NK.Admin

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
8	Integrity	HMAC with SHA-{1, 256} (IKE, IPsec)	FIPS180-4 [26] (SHA), RFC 2104 [50] (HMAC), RFC 2404 [40], RF C4868 [41], RFC 5996 [36] (IKEv2)	160, 256	FCS_COP.1/ NK.HMAC
9	Integrity	HMAC with SHA-{1, 256, 384} (TLS)	FIPS180-4 [26] (SHA), RFC 2104 [50] (HMAC), RFC 4346 [29] (TLSv1.1), RFC 5246 [30] (TLSv1.2)	160, 256, 384	FTP_TRP.1/ NK.Admin
10	Authenticated Encryption	AES in GCM mode (TLS)	FIPS180-4 [26] (SHA), SP800-38D [61] (GCM), RFC 5288 [55] (GCM for TLS), RFC 5116 [56] (AEAD), RFC 5246 [30] (TLSv1.2)	128, 256	FTP_TRP.1/ NK.Admin
11	Trusted Channel	IKEv2, IPsec	RFC 5996 [36], RFC 7296 [48] (IKEv2) RFC 4301 [31] (IPsec), RFC 4303 [34] (ESP)		FTP_ITC.1/ NK.VPN_TI, FTP_ITC.1/ NK.VPN_SIS
12	Trusted Channel	TLS v1.1 and v1.2	RFC 4346 [29] (TLSv1.1), RFC 5246 [30] (TLSv1.2)		FTP_TRP.1/ NK.Admin

Tabelle A.1: Kryptographische Funktionalitäten

No.	**Purpose**	**Cryptographic Mechanism**	**Standard of Implementation**	**Key Size in Bits**	**Security Level above 100 Bits**	**Comment**
1	Authenticity	RSA signature verification with encoding RSASSA-PKCS1-1.5 using SHA-256	RFC 3447 [25] (RSA), FIPS180-4 [26] (SHA)	4096	yes	Firmware update signatures verification FDP_ITC.1/ NK.FWUpdate

Tabelle A.2: Kryptographische Funktionalitäten (Aktualisierung)

Literaturverzeichnis

[1] Common Criteria, 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, 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, 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, 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 Interpretation 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

[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)

[10] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) geändert worden ist – SigG 2009)

[11] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die zuletzt durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) geändert worden ist – SigV 2010)

[12] Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29.07.2009 (BGBl. I, S. 2254), durch Artikel 5 des Gesetzes vom 29.07.2009 (BGBl. I, S. 2355 [2384] und durch Gesetz vom 14.08.2009 (BGBl. I, S. 2814)

[13] Common Criteria Protection Profile: Card Operating System (PP COS), BSI-CC-PP-0082, Version 1.0 vom 30.5.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[14] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.19, 03.12.2015, Technische Arbeitsgruppe TR-03116-1, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2018-01, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[16] Einführung der Gesundheitskarte: Spezifikation Konnektor [gemSpec_Kon], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 4.11.1, 27.04.2017

[17] Einführung der Gesundheitskarte: Übergreifende Spezifikation Netzwerk [gemSpec_Net], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 1.12.0, 18.12.2017

[18] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.9.0, 19.12.2017

[19] Einführung der Gesundheitskarte: Spezifikation des Card Operating System (COS) Elektrische Schnittstelle, Version 3.10.0, 21.04.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[20] Einführung der Gesundheitskarte: Spezifikation der gSMC-K / Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.10.0, 28.10.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[21] Einführung der Gesundheitskarte: Spezifikation: Festlegung von OIDs, Version 3.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[22] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation PKI, Version 2.1.0, 18.12.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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

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

[25] J. Jonsson, B. Kaliski: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. February 2003. RFC 3447, https://www.ietf.org/rfc/rfc3447.txt

[26] NIST: FIPS PUB 180-4 Secure Hash Signature Standard (SHS), August 2015, http://dx.doi.org/10.6028/NIST.FIPS.180-4

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

[28] NIST FIPS 197: Advanced Encryption Standard (AES). November 2001, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[29] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.1, April 2006, RFC 4346, http://www.ietf.org/rfc/rfc4346.txt

[30] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.2, August 2008, RFC 5246, http://www.ietf.org/rfc/rfc5246.txt

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

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

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

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

[35] C. Kaufman (Ed.): Internet Key Exchange (IKEv2) Protocol, December 2005, RFC 4306 (IKEv2), http://www.ietf.org/rfc/rfc4306.txt

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

[37] D. Black, D. McGrew: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, August 2008, RFC 5282, http://www.ietf.org/rfc/rfc5282.txt

[38] 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

[39] 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

[40] 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

[41] 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`

[42] 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`

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

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

[45] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose: Protocol Modifications for the DNS Security Extensions. March 2005, RFC 4035, `http://www.ietf.org/rfc/rfc4035.txt`

[46] R. Housley: Cryptographic Message Syntax, September 2009, RFC 5652, `http://www.ietf.org/rfc/rfc5652.txt`

[47] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), BSI-CC-PP-0047, Version 3.2.2 vom 11.04.2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[48] C. Kaufman et. al, RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, RFC 7296, `https://tools.ietf.org/html/rfc7296`

[49] D. Cooper et. al, RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, RFC 5280, `https://www.ietf.org/rfc/rfc5280.txt`

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

[51] Rivest, R., The MD5 Message-Digest Algorithm, April 1992.

[52] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller, May 2006

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

[54] Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), J. Merkle, M. Lochter, October 2013

[55] AES Galois Counter Mode (GCM) Cipher Suites for TLS, J. Salowey, A. Choudhury, D. McGrew, August 2008

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

[57] gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Übergreifende Spezifikation Operations und Maintenance, Version 1.8.0, 06.02.2017

[58] T-Systems International GmbH. Produkthandbuch T-Systems Konnektor, Version 1.30, 2019.

[59] T-Systems International GmbH. Schnittstellenspezifikation T-Systems Netzkonnektor, Version 1.6, 2018.

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

[61] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[62] HMAC-based Extract-and-Expand Key Derivation Function (HKDF), H. Krawczyk, P. Eronen, Mai 2010