Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen

Schutzprofil 1:
Anforderungen an den Netzkonnektor (NK-PP)

Common Criteria

BSI-CC-PP-0033

Freigegeben durch
das Bundesministerium für Gesundheit

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Einführung

Dieses Dokument ist durch das Bundesamt für Sicherheit in der Informationstechnik herausgegeben und repräsentiert das Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen, Schutzprofil 1: „Anforderungen an den Netzkonnektor (NK-PP)“. Das Schutzprofil entspricht den Anforderungen und dem Format der Gemeinsamen Kriterien Version 2.3 [1], [2], [3] mit relevanten finalen Interpretation der CCIMB.

Alle Zuschriften und Kommentare bzgl. dieses Schutzprofils sind an die folgende Adresse zu schicken:

KONTAKTADRESSE

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn
Tel +49 228 9582-0
Fax +49 228 9582-400
Email bsi@bsi.bund.de

Inhaltsverzeichnis

1. PP-Einführung

1.1. PP-Identifikation

Titel:	Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP)
Version des Dokuments:	1.05
Datum des Dokuments:	04.09.2007
Allgemeiner Status:	Final
Registrierung:	BSI-CC-PP-0033
Registrierung bei:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC-Version	2.3
Vertrauenswürdigkeitsstufe:	EAL4+
Auftraggeber und Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Verfasser:	Volker Schenk Prüfstelle IT-Sicherheit der T-Systems GEI GmbH
Stichwörter:	Konnektor, Netzkonnektor, eHealth, elektronisches Gesundheitswesen, Telematikinfrastruktur, dezentrale Komponente

Dieses Schutzprofil wurde erstellt auf der Grundlage folgender Dokumente:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Version 2.3, August 2005, CCMB-2005-08-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

In Abschnitt 5.1.1.5 wird für die Definition der Anforderung FPT_EMSEC.1 auf das folgende Schutzprofil verwiesen:

[14] Common Criteria Protection Profile – Secure Signature-Creation Device (SSCD) Type 3, CEN/ISSS by ESIGN Workshop – Expert Group F, Version 1.05, 25 July 2001, registered as BSI-PP-0006-2002

In Abschnitt 5.2.1 wird für die Definition der Anforderung FCS_RND.1/Env auf das folgende Schutzprofil verwiesen:

[13] Common Criteria Protection Profile Secure Module Card (PP-SMC), Version 1.0, 01.02.2006, BSI-PP-0019, Bundesamt für Sicherheit in der Informationstechnik

1.2. PP-Übersicht

Dieses Schutzprofil beschreibt den Schutzbedarf für einen Netzkonnektor im elektronischen Gesundheitswesen. Zu den gesetzlichen Grundlagen siehe Abschnitt 7.1 *Gesetzliche Anforderungen* im Anhang.

Ein Konnektor ist eine Rechnerplattform mit u.a. Paketfilter- und VPN-Funktionalität (Netzkonnektor) und sicherheitskritischen Anwendungskomponenten (Anwendungskonnektor mit Signaturanwendungskomponente). Die allgemeinen Funktionen und Schnittstellen des Konnektors sind in der Konnektor-Spezifikation [20] beschrieben. Der Netzkonnektor stellt einen Teil des Konnektors dar; die genaue Abgrenzung wird im Folgenden näher beschrieben (siehe Abschnitte 1.2.2 und 1.2.3). Dieses Schutzprofil extrahiert einige sich aus der Konnektor-Spezifikation [20] ergebende Sicherheitsanforderungen an den Netzkonnektor und stellt die Grundlage für die Evaluierung und Zertifizierung von Netzkonnektoren dar.

1.2.1. Terminologie

Der Konnektor bildet die Schnittstelle zwischen der zentralen **Telematikinfrastruktur** des Gesundheitswesens[1] und den Primärsystemen des Gesundheitswesens. Die Chipkarten elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA) und Berufsausweis (BA) sowie die Sicherheitsmodule (SMC, Secure Module Card), die Konnektoren, die Kartenterminals, die Sicherheitsmodule für den Netzkonnektor (SM-K) und die Kartenterminals (SM-KT), die Kommunikationsinfrastruktur und die Dienste bilden zusammen die Telematikinfrastruktur. Zu den Primärsystemen gehören die Praxisverwaltungssysteme der Ärzte (PVS), die Krankenhausinformationssysteme (KIS) und die Apothekenverwaltungssysteme (AVS). Die lokal in den Räumlichkeiten der Leistungserbringer installierten Komponenten werden **dezentrale Komponenten der Telematikinfrastruktur** (oder auch: Komponenten der dezentralen Telematikinfrastruktur) genannt. Neben den Konnektoren stellen auch die Kartenterminals sowie die Chipkarten elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA), Berufsausweis (BA) und Secure Module Card (SMC) dezentrale Komponenten dar.

Audit-Daten vs. Logging: In der Begriffswelt des elektronischen Gesundheitswesens wird mit dem Ausdruck „Audit-Daten“ häufig der zentrale Audit-Dienst in der Telematikinfrastruktur bezeichnet. Der Begriff Audit-Daten wird in diesem Schutzprofil auch im Sinne der Common Criteria verwendet. Im Sinne der Common Criteria bezeichnet dieser Begriff ganz allgemein Anforderungen aus der Klasse FAU (Security Audit), die im elektronischen Gesundheitswesen eher mit „Logging“ bezeichnet würden. Dieses Schutzprofil verwendet ebenfalls den Begriff „Logging“, wo dies möglich ist, nutzt aber auch den Begriff „Audit“, wenn z.B. funktionale Anforderungen aus den Common Criteria zitiert werden.

---

[1] Ein Glossar befindet sich in Anhang in Abschnitt 7.3. Für Fachtermini der elektronischen Gesundheitskarte und der Telematikinfrastruktur des Gesundheitswesens wird darüber hinaus auf „Die Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, Projektinternes Glossar, Version 1.0 vom 14. März 2005“ verwiesen. Dieses und weitere Dokumente sind in elektronischer Form zu finden auf den Seiten des DIMDI, http://www.dimdi.de, Stichwörter eHealth / Gesundheitskarte. Ferner gibt es ein Projekt-Glossar der gematik, siehe [31].

Die Funktionalität, die üblicherweise unter dem Begriff „Audit“ verstanden wird, wird hier durch O.Protokoll sowie durch das Stichwort Ereignisprotokollierung im Abschnitt Selbstschutz gefordert. Die Modellierung der zustandsgesteuerten Filterung erfolgt durch das Ziel O.Stateful und die Anforderung FAU_GEN.1/Stateful im Abschnitt 5.1.1.4 Stateful Packet Inspection.

Zeitstempel: Der Begriff Zeitstempel wird in diesem Schutzprofil im Sinne der Common Criteria verwendet. Er bezeichnet eine Kombination aus aktuellem Datum und aktueller Uhrzeit. Die Forderung nach einem Zeitstempel (vgl. die funktionale Anforderung FPT_STM.1/TOE in Abschnitt 5.1.1.3) impliziert, dass der Zeitstempel von einer EVG-eigenen Echtzeituhr bezogen wird und dass beispielsweise Log-Einträgen ein aktuelles Datum mit aktueller Uhrzeit hinzugefügt werden kann. Diese Verwendung des Begriffs „Zeitstempel“ impliziert keine Signatur der Daten (insbesondere auch keine qualifizierte Signatur) und auch keine netzbasierten Zeitstempeldienst, sondern ist auf die Bereitstellung hinreichend exakter Informationen zu Datum und Uhrzeit beschränkt.

Informationsflusskontrolle/Anwendungslogik (IFK/AL) und Signaturanwendungskomponente (SAK, siehe auch den folgenden Abschnitt 1.2.2) werden zusammen häufig als **Anwendungskonnektor** bezeichnet (im Gegensatz zum Netzkonnektor). In der Literatur wird der Begriff Anwendungskonnektor allerdings auch als Synonym für IFK/AL verwendet. Letztlich hat es sich im Sprachgebrauch durchgesetzt, sowohl IFK/AL ohne SAK als auch IFK/AL mit SAK als Anwendungskonnektor zu bezeichnen. In diesem Schutzprofil wird, wo es zur Klarstellung erforderlich ist, vom Anwendungskonnektor im engeren Sinne (IFK/AL ohne SAK, abgekürzt: AK i.e.S.) und vom Anwendungskonnektor im weiteren Sinne (IFK/AL mit SAK, abgekürzt: AK i.w.S.) gesprochen.

1.2.2. Funktionsblöcke des Konnektors

Der Konnektor erbringt Sicherheitsleistungen in drei wesentlichen Funktionsblöcken:

- Er ermöglicht die sichere Anbindung der dezentralen Komponenten an die zentralen Dienste der Telematikinfrastruktur Dieser Aspekt beinhaltet unter anderem Funktionalitäten eines dynamischen Paketfilters und eines VPN-Clients und wird „**Netzkonnektor**“ genannt (abgekürzt: NK).

  Während des Aufbaus des gesicherten Kanals ermöglicht der Netzkonnektor die Authentisierung dezentraler und zentraler Komponenten. Er schützt sich selbst und die Primärsysteme vor Angriffen aus offenen[2] Netzen.[3] Der gesicherte Kanal wird in Form eines virtuellen privaten Netzes (virtual private network, VPN) realisiert, der als Übertragungsmedium offene Netze (z.B. das Internet, meist neutral „Transportnetz“ genannt) nutzen kann. Indem der Netzkonnektor *zu schützende Daten*[4] korrekt

[2] „offen“ hier im Sinne von öffentlich zugänglich und ungeschützt

[3] Dieser Schutz kann durch den Netzkonnektor nur dann geleistet werden, wenn es keine weiteren Verbindungen zwischen den Primärsystemen und dem Transportnetz gibt. Siehe auch Annahme A.Betrieb_AK in Abschnitt 3.6.

[4] siehe Abschnitt 3.1

weiterleitet (Routing, erzwungene Nutzung des VPN-Kanals), trägt er auch zu einer Informationsflusskontrolle bei.

- Er steuert die lokalen Abläufe, einschließlich der Ablaufsteuerung von offline-Geschäftsvorfällen[5], und kontrolliert die Informationsflüsse zwischen den lokalen Netzen der Leistungserbringer und den zentralen Diensten („**Informationsflusskontrolle und Anwendungslogik**“, abgekürzt: IFK/AL).

  Er ermöglicht die Kommunikation zwischen den Komponenten (Primärsystem, Kartenterminals mit eGK und HBA) im lokalen Netzwerk der Leistungserbringer sowie die Datenübertragung zwischen den Primärsystemen und der Telematikinfrastruktur über den gesicherten Kanal und überwacht gleichzeitig die Zulässigkeit von Informationsflüssen. Er stellt sicher, dass *zu schützende Daten* nur verschlüsselt bzw. signiert übertragen werden. Damit trägt er zum Schutz medizinischer und personenbezogener Daten bei. Er ermöglicht den Aufbau von gesicherten Verbindungen[6] zu Kartenterminals und von gesicherten direkten Verbindungen zwischen Chipkarten[7].

- Er beinhaltet eine **Signaturanwendungskomponente** (abgekürzt: SAK), um die im Rahmen der Abläufe geforderten qualifizierten Signaturen[8] erstellen und prüfen zu können.

  Der Konnektor erbringt Sicherheitsdienste einer Signaturanwendungskomponente, welche mit Hilfe von Chipkarten fortgeschrittene (eGK) und qualifizierte (HBA) elektronische Signaturen erstellt und verifiziert sowie Daten verschlüsselt und entschlüsselt. Er stellt für die dezentralen Systeme Zeitstempel bereit.[9]

Der Konnektor erfüllt die relevanten Anforderungen des **Bundesdatenschutzgesetzes** (BDSG [10]) sowie des **Signaturgesetzes** und der **Signaturverordnung** (SigG 2001 [7] bzw. SigV 2001 [8]):

- Bei medizinischen Daten von Versicherten und bei Versichertenstammdaten handelt es sich um personenbezogene Daten im Sinne des §3 (1) BDSG, die gemäß §3 (4) BDSG durch den Konnektor verarbeitet werden.
- Der Teil des Anwendungskonnektors im weiteren Sinne, der mit dem Prozess des Erzeugens und Prüfens (Verifizierens) von qualifizierten Signaturen sowie mit der Darstellung von zu signierenden Daten befasst ist, erfüllt die Anforderungen an Signaturanwendungskomponenten gemäß SigG und SigV.

---

5 Auch bei Ausfall der online-Netzverbindung zu den zentralen Diensten der Telematikinfrastruktur sollen Geschäftsvorfälle – zumindest in eingeschränktem Funktionsumfang – lokal (offline) durch den Konnektor bearbeitet werden können.

6 unter Nutzung des TLS-Protokolls

7 unter Nutzung von Secure Messaging gemäß ISO/IEC 7816 [55] nach vorangegangener Card-to-Card-Authentisierung

8 beispielsweise: Signatur des Arztes beim Ausstellen eines eRezepts

9 Hierbei handelt es sich nicht um qualifizierte Zeitstempel.

- Der Konnektor macht sicherheitstechnische Veränderungen des Konnektors für den Anwender erkennbar[10].

Application Note 1: Diese oben genannten Anforderungen beziehen sich auf den Konnektor als Ganzes. Die Anforderungen für den Netzkonnektor, der Gegenstand dieses Schutzprofils ist, werden im Verlauf dieses Schutzprofils präzisiert.

Application Note 2: **Mechanismen zum Integritätsschutz:** Der Konnektor muss keinen Schutz vor Hardware-Manipulationen bieten (siehe Annahme A.phys_Schutz in Abschnitt 3.6 und Application Note 4: *Möglichkeit zur Differenzierung*), wohl aber Mechanismen zum Integritätsschutz seiner Software implementieren. Siehe auch die Anforderung FPT_TST.1 und Application Note 88:.

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

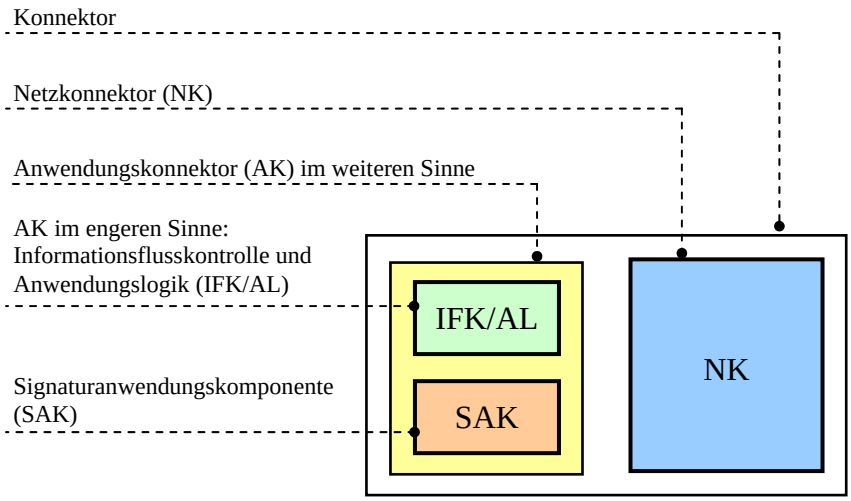

Abbildung 1: Funktionsblöcke des Konnektors

1.2.3. Unterteilung in vier Schutzprofile

In Anlehnung an die in Abbildung 1: Funktionsblöcke des Konnektors beschriebene Unterteilung in Netzkonnektor (NK), Informationsflusskontrolle und Anwendungslogik (IFK/AL) und Signaturanwendungskomponente (SAK) und unter Berücksichtigung der Tatsache, dass der Netzkonnektor zusätzlich über ein Sicherheitsmodul (SM-K) verfügt (vgl. Annahme A.SM-K), wurden die Sicherheitsanforderungen an den Konnektor in vier getrennten Schutzprofilen formuliert:

- Schutzprofil für den Netzkonnektor (NK-PP),
- Schutzprofil für den Anwendungskonnektor bzw. die Informationsflusskontrolle und Anwendungslogik IFK/AL (AK-PP), und

[10] vgl. §15 Abs. 4 SigV: Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

- Schutzprofil für die Signaturanwendungskomponente des Konnektors (SAK).
- Ferner wird ein weiteres Schutzprofil die Anforderungen an das Sicherheitsmodul für den Netzkonnektor (SM-K) sowie das in SICCT-Kartenterminals einzusetzende Sicherheitsmodul (SM-KT) formulieren.

Dabei wurde versucht, möglichst viele Teile in den Schutzprofilen identisch zu halten, so dass die Evaluierung eines Produktes, welches alle Funktionsblöcke implementiert, leicht durchführbar ist.

Das vorliegende Dokument stellt das Schutzprofil für den Netzkonnektor (NK-PP) dar.

1.3. Konformität / Postulat der Übereinstimmung mit den CC

1.3.1. Common Criteria Konformität

Das Schutzprofil wurde gemäß Common Criteria Version 2.3 (entspricht im wesentlichen Common Criteria Version 2.1 oder Version 2.2 jeweils mit allen Final Interpretations[11]) erstellt.

Es wurde eine funktionale Sicherheitsanforderung (FPT_EMSEC.1, siehe Abschnitt 6.3.1) definiert, die nicht in CC Teil 2 [2] enthalten ist. Ferner wurde an die IT-Einsatzumgebung des Evaluationsgegenstands mit FCS_RND.1/Env (vgl. Abschnitt 5.2.1) eine Anforderung formuliert, die ebenfalls explizit dargelegt ist (explicitly stated). Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [3] entnommen.

Daher ist dieses Schutzprofil:

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

1.3.2. Schutzprofil-Konformität

Dieses Schutzprofil behauptet keine Konformität zu einem anderen Schutzprofil.

1.3.3. Paket-Konformität

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe **EAL4**, **augmentiert um die Komponenten ADV_IMP.2, AVA_MSU.3 und AVA_VLA.4** (im Folgenden bezeichnet mit „EAL4+“).

[11] Eine aktuelle Liste der Final Interpretations findet sich unter http://www.commoncriteriaportal.org.

1.4. PP-Organisation

Der Aufbau dieses Schutzprofils folgt der Mustergliederung, die durch *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model* [1], Anhang A, vorgegeben wird.

1.5. Hinweise zur Anwendung des PPs auf unterschiedliche Ausprägungen des EVGs

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

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

Gleichzeitig wurden die Annahmen möglichst vollständig formuliert, damit im ST im Vergleich zum Schutzprofil keine zusätzlichen Annahmen aufgenommen werden müssen.[12] Es steht dem ST-Autor jederzeit frei, in Form von Annahmen formulierte Sicherheitsleistungen in EVG-Sicherheitsziele und -anforderungen umzuwandeln.

Siehe auch Application Note 3: (mögliche Einsatzumgebungen), Application Note 4: (Möglichkeit zur Differenzierung), Application Note 6: (Einbox- vs. Mehrbox-Lösung), und Application Note 7: (spezielle Einsatzumgebungen).

[12] Aus den Anforderungen der Common Criteria folgt, dass ein PP-konformes ST sämtliche EVG-Sicherheitsziele und -anforderungen aus dem PP übernehmen muss und keine zusätzlichen Annahmen an die Einsatzumgebung treffen darf, welche die Einsatzmöglichkeiten des EVGs einschränken.

2. EVG-Beschreibung: Der Netzkonnektor

Der Netzkonnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur des Gesundheitswesens (außerhalb der Verantwortlichkeit des Leistungserbringers) und den dezentralen Systemen. Er stellt den netzseitigen Abschluss der Telematikinfrastruktur dar. Die Verantwortung für den Betrieb des Netzkonnektors liegt beim Leistungserbringer; der Netzkonnektor stellt jedoch ein Zugangserfordernis zur Telematikinfrastruktur dar und es dürfen nur von der Gematik zugelassene und geprüfte Konnektoren eingesetzt werden.

Die Situation ist vergleichbar mit der Bereitstellung eines ISDN-Telefon-Festnetzanschlusses durch einen Netzbetreiber, dessen Zuständigkeit an definierter Stelle endet, z.B. am Netzwerkterminator (NTBA[13]).

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

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

Der VPN-Kanal (siehe FTP_ITC.1/VPN) stellt eine Absicherung der Kommunikationsbeziehung zwischen Netzkonnektor und VPN-Konzentrator auf unterer Ebene dar. Nach erfolgtem Aufbau des VPN-Kanals durch den Netzkonnektor (= EVG) nutzt der Anwendungskonnektor (= IT-Umgebung) diesen Kanal und authentisiert[14] die Organisation des Leistungserbringers gegenüber dem Broker (der danach den Zugriff auf die Fachdienste der zentralen Telematikinfrastruktur erlaubt). Dazu nutzt der Anwendungskonnektor Schlüsselmaterial, welches auf einem der Organisation des Leistungserbringers zugeordneten Sicherheitsmodul (**SMC Typ B**) gespeichert ist. Anschließend wird mittels TLS (Transport Layer Security) ein sicherer Kanal zwischen Anwendungskonnektor und zentralen Diensten aufgebaut. Der Anwendungskonnektor und der sichere TLS-Kanal sind nicht Teil des EVGs. – Die über den TLS-Kanal transportierten Daten werden teilweise auf Anwendungsebene weiter geschützt, beispielsweise durch mit einem HBA erstellte Signaturen. Auch diese Funktionalität ist nicht Teil des EVGs.

Die gematik überwacht die Zulassung von Konnektoren und Kartenterminals durch die Erteilung von Bauartzulassungen. Das Vorliegen einer Bauartzulassung für einen Netzkonnektor wird durch ein entsprechendes Zertifikat im zugehörigen SM-K nachgewiesen. Die Verantwortung für den Einsatz und Betrieb der dezentralen Komponenten HBA, SMC und Kartenterminal liegt beim Leistungserbringer. Die unabhängige Prüfung (Evaluierung und Zertifizierung gemäß Common Criteria) der im Gesundheitswesen eingesetzten

[13] Network Termination for ISDN Basic rate Access

[14] Diese Authentisierung ist nicht Gegenstand des Schutzprofils; vgl. dazu im *Common Criteria Protection Profile Secure Module Card (PP-SMC)* [13] den *Service_Client_Server_Auth*.

Komponenten bildet eine Vertrauensbasis für die beteiligten Stellen. Für den Netzkonnektor muss die Prüfung nach dem Dokument „Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP)“ (=dieses vorliegende Dokument) erfolgen.

2.1. Einsatzumgebung des Konnektors

Der Netzkonnektor stellt einen Teil des Konnektors dar (siehe Abbildung 1 in Abschnitt 1.2.2 Funktionsblöcke des Konnektors). Seine Aufgabe ist es, die Verbindung zwischen dezentralen und zentralen Komponenten herzustellen. Der Netzkonnektor kommuniziert daher mit dem Anwendungskonnektor bzw. mit dem lokalen Netz und mit der über WAN angebundenen zentralen Telematikinfrastruktur.

Application Note 3: Der ST-Autor soll die Einsatzumgebung des Netzkonnektors in seiner konkreten Ausprägung beschreiben (Einbox- oder Mehrkomponentenlösung).

Die Einsatzumgebung des Konnektors im allgemeinsten Fall (Mehrkomponentenlösung) ist in der folgenden Abbildung 2 dargestellt; Einbox-Lösungen werden danach diskutiert (vgl. Abbildung 3). Diese Abbildungen sollen lediglich beispielhaft mögliche Ausprägungen der Einsatzumgebung darstellen. Es sind weitere Variationen möglich; der ST-Autor soll die konkrete Ausprägung für sein Produkt beschreiben.

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

Mit gestrichelten Linien dargestellte Komponenten bzw. Verbindungen sind optional – in den folgenden Abbildungen sind dies optionale weitere VPN-Konzentratoren für Mehrwertdienste.

Alle Teilkomponenten des Konnektors werden durch dicke schwarze Rahmen gekennzeichnet. Der Netzkonnektor als ein Teil des Konnektors ist durch blaue Färbung bzw. Schattierung kenntlich gemacht. Der Netzkonnektor stellt den EVG dar – durch die blaue Schattierung wird also die physikalische EVG-Abgrenzung beschrieben. Mit roten Linien werden zum besseren Verständnis Komponenten zusammengefasst, die üblicherweise in einem gemeinsamen Gehäuse untergebracht sind (insbesondere bei der Einbox-Lösung) oder die auf einer gemeinsamen Plattform ablaufen (z.B. Hardware des Primärsystems). Abhängig vom Einsatzszenario können die roten Linien geschützten Bereichen (vgl. A.phys_Schutz) entsprechen. Der ST-Autor soll durch die Einsatzumgebung zu schützende Bereiche geeignet kenntlich machen.

Neben den dargestellten physikalischen Verbindungen gibt es logische Kanäle, die über die physikalischen Verbindungen etabliert werden und üblicherweise zusätzlich geschützt werden (sichere Kanäle). Dies sind (i) die Verbindung zwischen SAK bzw. Trusted Viewer und der Darstellungskomponente des Trusted Viewers sowie (ii) die Verbindung zwischen den Kartenterminals (SICCT) und dem Anwendungskonnektor. Diese Verbindungen sind in den folgenden Abbildungen aus Gründen der Übersichtlichkeit nicht dargestellt.

Außerdem abstrahieren die folgenden Abbildungen von der Tatsache, dass die SMC Typ B auf verschiedenste Arten an den Anwendungskonnektor angebunden werden kann – etwa mittels eines per LAN angebundenen Kartenterminals. Die SMC Typ B wurde daher in allen Abbildungen direkt dem Anwendungskonnektor zugeordnet.

In den folgenden Abbildungen bedeuten die Abkürzungen:

- AK: Anwendungskonnektor im engeren Sinne (IFK/AL)
- TV: Trusted Viewer, sichere Anzeigekomponente der SAK
- Darstell.komp.TV: Darstellungskomponente des Trusted Viewers
- SICCT (=Secure Interoperable Chip Card Terminal): Kartenterminal; in den folgenden Abbildungen ist aus Gründen der Übersichtlichkeit stets nur ein Kartenterminal dargestellt
- Paketfilter: LAN-seitiger Paketfilter zum Schutz des AK. Die spitze Seite des Paketfilter-Symbols zeigt jeweils zu der Seite, von der potentielle Angriffe abgewehrt werden sollen. Innerhalb des Netzkonnektors ist symbolhaft angedeutet, welchen Schutz der Netzkonnektor in den jeweiligen Szenarien für den Anwendungskonnektor zur Verfügung stellt. Unabhängig davon besitzt der Netzkonnektor stets einen LAN-seitigen Paketfilter, der ihn selbst vor potentiellen Angriffen aus dem LAN schützt. Dieser Aspekt wird in den folgenden Abbildungen nicht symbolhaft dargestellt – die Abbildungen sollen deutlich machen, dass der Netzkonnektor im Fall der Einbox-Lösung über die zusätzliche Sicherheitsfunktionalität „Schutz des Anwendungskonnektors vor potentiellen Angriffen aus dem LAN“ verfügt (vgl. auch O.PF_LAN und Abschnitt 7.6.19).
- Primärsystem-HW: Hardware des Primärsystems. Auf dieser Plattform läuft die Software des Leistungserbringers (z.B. Praxisverwaltungssystem, Apothekenverwaltungssystem, Krankenhaus-Informationssystem). Im Allgemeinen wird dort auch die Darstellungskomponente des Trusted Viewers ablaufen.
- PVS: Praxis-Verwaltungssystem. Dieser Ausdruck steht stellvertretend auch für Apotheken-Verwaltungssysteme (AVS) oder Krankenhaus-Informationssysteme (KIS). Er bezeichnet den Softwareanteil auf dem Primärsystem. Das Betriebssystem des Primärsystems ist in den folgenden Abbildungen nicht dargestellt.

Die übrigen verwendeten Abkürzungen sind im Abkürzungsverzeichnis in Abschnitt 7.2 erläutert.

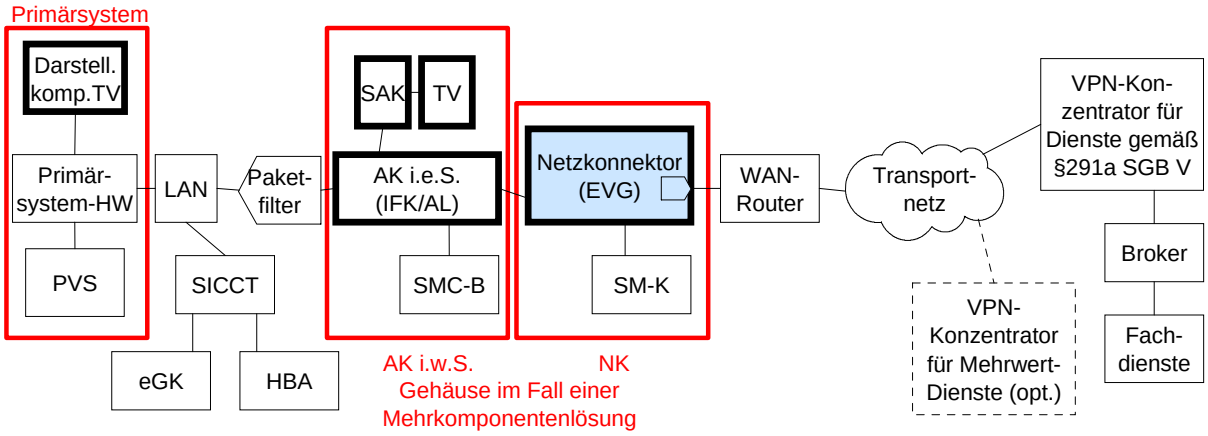

Abbildung 2: Einsatzumgebung des Konnektors, Mehrkomponentenlösung
(ein zusätzlicher Paketfilter schützt den AK)

Der WAN-Router kann mit dem Netzkonnektor in einem gemeinsamen Gehäuse integriert sein, ist aber nicht notwendigerweise Teil[15] des Netzkonnektors im Sinne dieses Schutzprofils. WAN-Router-Funktionalität kann z.B. mit einem DSL-Modem integriert werden. In jedem Fall besitzt der WAN-Router keine Sicherheits-funktionalität. Der ST-Autor soll eine exakte physikalische und logische Abgrenzung des EVG vornehmen und beschreiben, ob und ggf. welche Funktionalitäten der EVG zusätzlich zu den Sicherheitsfunktionalitäten bietet.

Auch im Fall einer Mehrkomponentenlösung muss der Anwendungskonnektor vor Angriffen aus dem LAN geschützt werden. Dieser Schutz muss aber nicht durch den Netzkonnektor geleistet werden. Falls der Netzkonnektor dies nicht leistet, muss eine zusätzliche Komponente eingesetzt werden, welche gleichwertige Sicherheit bietet. In Abbildung 2 wird diese Komponente mit dem Begriff „Paketfilter“ bezeichnet.

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

Für den Fall der Einbox-Lösung ergibt sich z.B. folgendes Bild:

[15] Der WAN-Router muss auch bei Integration in einem Gehäuse, auf einer Platine oder in einer Baugruppe mit dem (Netz-)Konnektor keinen Teil des Konnektors darstellen in dem Sinne, dass er keine Sicherheitsfunktionalität bereitstellt. Vielmehr handelt es sich dann um ein multifunktionales Gerät, bei dem ein Konnektor (gemäss den Konnektor-Schutzprofilen) und ein WAN-Router „zufällig“ denselben Raum einnehmen. Es ist zulässig, dass ein integrierter WAN-Router im ST physikalisch als nicht zum EVG gehörig abgegrenzt wird.

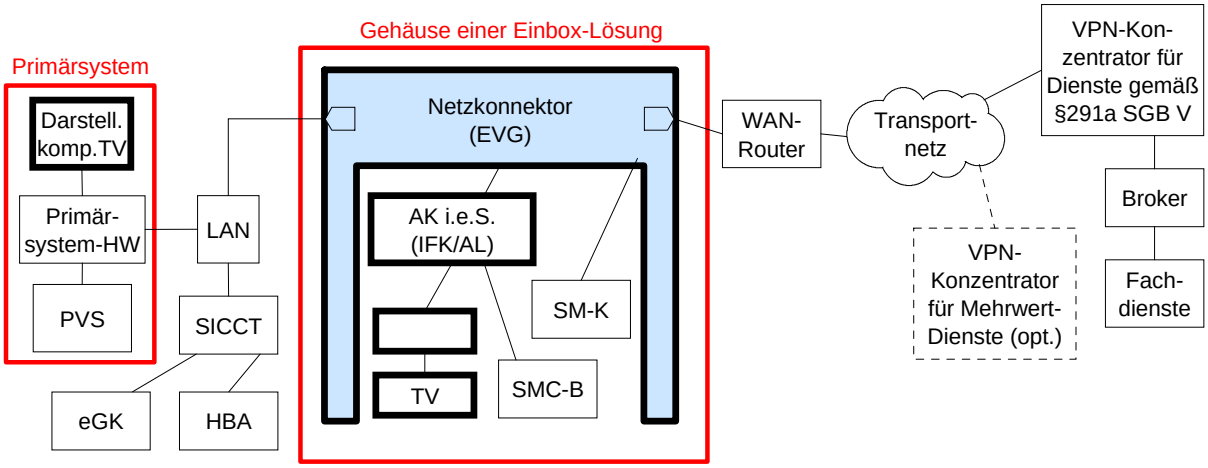

Abbildung 3: Einsatzumgebung des Konnektors, Einbox-Lösung
(der LAN-seitige Paketfilter des NK schützt den AK)

Auf eine zusätzliche Firewall zum Schutz des Anwendungskonnektor vor Angriffen aus dem LAN kann hier verzichtet werden, da der Netzkonnektor den Anwendungskonnektor vor solchen Angriffen schützt.

Falls der Netzkonnektor als Einbox-Lösung ausgestaltet ist, wird vom Netzkonnektor gefordert, dass er den Anwendungskonnektor vor Angriffen aus dem LAN schützt (siehe auch Sicherheitsdienst (2) (a) in Abschnitt 2.4 und Application Note 20: sowie Abschnitt 7.6.19).

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

Der ST-Autor muss im Security Target die Einsatzumgebung eindeutig beschreiben. Er sollte dazu eine Skizze erstellen, vergleichbar zu Abbildung 2 oder Abbildung 3. Die Skizze muss geeignet sein, die physikalischen und logischen Schnittstellen zwischen dem EVG und seiner IT-Umgebung zu erkennen. Abhängig von der konkreten Ausprägung des Produkts ist die Beschreibung der Schnittstellen in Abschnitt 2.2 geeignet anzupassen.

Es wird angenommen, dass die Einsatzumgebung des Netzkonnektors diesen vor physischen Angriffen schützt (siehe Annahme A.phys_Schutz in Abschnitt 3.6).

Application Note 4: **Möglichkeit zur Differenzierung:** Ein Hersteller kann sich mit seinem Produkt in diesem Punkt von Mitbewerbern differenzieren, indem sein Produkt Schutz vor physischen Angriffen bietet. In diesem Fall ist im Security Target das Sicherheitsziel für die Umgebung OE.phys_Schutz in ein Ziel für den EVG umzuwandeln und es sind geeignete funktionale Anforderungen an den EVG zu stellen (aus der Familie FPT_PHP). Der obige Satz kann dann im ST gestrichen werden.

Ein Leistungserbringer, der für den reibungslosen Betrieb in seiner Organisation verantwortlich ist, kann sich dann bewusst für ein solches Gerät entscheiden, um sein eigenes Risiko zu minimieren.

Vergleiche zu diesem Themenkomplex auch

- Application Note 43: Differenzierung durch physischen Schutz und
- Application Note 49: Annahmen zum physischen Schutz.

Es wird angenommen, dass die Primärsysteme in sicherer Weise an potentiell unsichere Netze (z.B. Internet) angebunden sind. Ferner wird angenommen, dass die Primärsysteme nach dem aktuellen Stand der Technik entwickelt wurden und administriert werden, so dass sie das spezifizierte Verhalten zeigen. Für Details siehe Annahme A.Betrieb_AK in Abschnitt 3.6.

Application Note 5: Dies kann beispielsweise dadurch erreicht werden, dass von den Primärsystemen außer der Verbindung über den Netzkonnektor keine weiteren Verbindungen in potentiell unsichere Netze existieren. Der ST-Autor soll beschreiben, ob und ggf. welche speziellen Annahmen getroffen werden.

Es muss davon ausgegangen werden, dass sich auf einem Primärsystem auch schadhafte (bösartige) Software befinden kann.

Application Note 6: **Einbox- vs. Mehrbox-Lösung:** In Abbildung 3 ist der Fall einer Einbox-Lösung für den Konnektor dargestellt. Es ist grundsätzlich nicht ausgeschlossen, Anwendungskonnektor und Netzkonnektor auf mehrere physische Einheiten zu verteilen bzw. als getrennte Produkte in jeweils eigenem Gehäuse zu gestalten.

Teilt ein Hersteller seinen Konnektor physisch auf mehrere Boxen auf, so muss er organisatorische oder technische Anforderungen für eine sichere Kommunikation zwischen den getrennten Teilen formulieren. Wird ein solcher sicherer Kanal kryptographisch implementiert, so ist ein geeignetes Schlüsselmanagement erforderlich (Schlüsselvereinbarung bzw. –austausch, sichere Schlüsselspeicherung). Siehe auch Abschnitt 7.6.3 Zuordnung der Basisdienste zu Konnektorteilen und Application Note 30: Einbox-Lösung sowie die Annahme A.phys_Schutz.

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

Application Note 7: **Spezielle Einsatzumgebungen:** Falls für ein Produkt der Einsatz in speziellen Umgebungen (z.B. Krankenhaus, mobiler Einsatz) geplant ist, soll dies im Security Target thematisiert werden. Aus den veränderten Einsatzbedingungen können sich zusätzliche spezifische Anforderungen ergeben.

2.2. Schnittstellen des Konnektors

2.2.1. Physische Schnittstellen des EVGs

Application Note 8: Der ST-Autor soll die Beschreibung der physischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Netzkonnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern.

Der EVG besitzt folgende physische Schnittstellen:

PS1 Eine Schnittstelle zum Anwendungskonnektor bzw. zum LAN.

Application Note 9: Die Schnittstelle zum Anwendungskonnektor kann unterschiedlich ausgeprägt sein:

- Im Fall einer Einbox-Lösung kann es eine interne Schnittstelle innerhalb der Box sein.
- Im Fall einer Mehrkomponentenlösung kann es sich auch um eine Schnittstelle zum lokalen Netzwerk (LAN) des Leistungserbringers handeln. Logisch kommuniziert der Netzkonnektor dann über diese Schnittstelle mit dem Anwendungskonnektor.
- Im Fall einer Einbox-Lösung muss der Paketfilter des Netzkonnektors den Anwendungskonnektor auch vor Angriffen aus dem LAN schützen. In diesem Fall stellt der Netzkonnektor dem Anwendungskonnektor zusätzlich eine physische Schnittstelle zum Primärsystem bereit (logisch kommuniziert der Netzkonnektor zwar nicht mit dem LAN oder den Primärsystemen, aber er stellt dem Anwendungskonnektor den Paketfilter bereit, wodurch sich eine zusätzliche physische Schnittstelle ergibt).
  Im Fall einer Einbox-Lösung kann sich daher die physische Schnittstelle PS1 aufspalten in zwei Schnittstellen: eine Schnittstelle zum Anwendungskonnektor (z.B. PS1a) und eine Schnittstelle zum LAN (z.B. PS1b).

Der ST-Autor soll beschreiben, über welche physischen Schnittstellen der EVG verfügt.

PS2 Eine Schnittstelle zu Datennetzen (WAN), welche als Transportnetz für den Zugang zur Telematikinfrastruktur dienen. Es wird angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und nicht notwendigerweise verschlüsselt sind.

Die mit PS1 bezeichnete LAN-Schnittstelle und die mit PS2 bezeichnete WAN-Schnittstelle sollten nicht in einer physischen Schnittstelle zusammenfallen.

Application Note 10: Falls die mit PS1 bezeichnete LAN-Schnittstelle und die mit PS2 bezeichnete WAN-Schnittstelle in einer physischen Schnittstelle zusammenfallen, muss der ST-Autor nachweisen, dass der Konnektor dennoch die Netze (LAN und WAN) sicher von einander trennt.

PS3 Eine möglicherweise proprietäre (herstellerspezifische) Wartungsschnittstelle für das lokale Management des Netzkonnektors.

Application Note 11: Die mit PS3 bezeichnete lokale Management-Schnittstelle kann auch mit PS1 zusammenfallen, d.h., eine gesonderte Schnittstelle ist weder erforderlich noch verboten. In Abbildung 2 und Abbildung 3 ist diese Schnittstelle nicht dargestellt.

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

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

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

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

Schließlich wird die **physische Hülle des Konnektors** als weitere Schnittstelle betrachtet, über die – abhängig von der angenommenen Einsatzumgebung – Angriffe vorgenommen werden können (siehe auch Abschnitt 7.6.7).

Application Note 12: Der ST-Autor soll die Schnittstellen nach Möglichkeit in Form einer Skizze grafisch darstellen. Dazu kann auch auf bereits in Abschnitt 2.1 enthaltene Abbildungen verwiesen werden.

2.2.2. Logische Schnittstellen des EVGs

Application Note 13: Der ST-Autor soll die Beschreibung der logischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Netzkonnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern.

Der EVG besitzt folgende logische Schnittstellen:

LS1 Eine Schnittstelle zur entfernten Telematikinfrastruktur, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS2) erreicht wird.

LS2 Eine Schnittstelle zum Anwendungskonnektor (via PS1).

LS3 Eine Schnittstelle zu den Primärsystemen, die physisch über das LAN (PS1) des Leistungserbringers erreichbar sind.

Application Note 14: Diese Schnittstelle ist insbesondere im Fall einer Einbox-Lösung vorhanden, bei welcher der Netzkonnektor den Anwendungskonnektor vor Angriffen aus dem LAN schützt. In anderen Produktausprägungen kann diese Schnittstelle entfallen.

LS4 Eine Schnittstelle zu einem Sicherheitsmodul für den Netzkonnektor (Secure Module Konnektor, SM-K) sowie optional zu weiteren Chipkarten (via PS4).

LS5 Eine Schnittstelle zu möglicherweise proprietären (herstellerspezifischen) lokalen Managementfunktionen des Netzkonnektors (via PS3 oder PS1).

2.3. Aufbau und physische Abgrenzung des Netzkonnektors

Zur Gesamtarchitektur und für einen Überblick über die Kernkonzepte sei auf die Konnektor-Spezifikation [20] in ihrer jeweils aktuellen Version verwiesen. Eine grobe Abgrenzung des Netzkonnektors von den übrigen Teilen des Konnektors erfolgte bereits in Abschnitt 1.2.2.

Application Note 15: Der ST-Autor soll in diesem Abschnitt die Architektur seines Produkts beschreiben. Dabei soll er sich an der aktuellen Version der Konnektor-Spezifikation [20] orientieren. Siehe auch die Hinweise in Abschnitt 7.6.3 und 7.6.4.

Der EVG verfügt über eine für den Benutzer leicht zugängliche Anzeige, die ihm die Betriebsbereitschaft sowie das Bestehen oder Nichtbestehen einer sicheren VPN-Verbindung zur zentralen Telematikinfrastruktur signalisiert.

2.4. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste

Application Note 16: Die im Folgenden beschriebene Sicherheitsfunktionalität stellt die Mindestanforderung an den Netzkonnektor dar: Ein Netzkonnektor (EVG), der dieses Schutzprofil erfüllt, muss mindestens diese Anforderungen erfüllen. Erbringt er darüber hinausgehende Leistungen, so dürfen sie die in diesem Schutzprofil geforderte Sicherheitsfunktionalität nicht beeinträchtigen.

Der EVG erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [20] definierten Schnittstellen weitgehend automatisch. Informationsflüsse werden grundsätzlich durch den Anwendungskonnektor initiiert. Der EVG erlaubt ein lokales Management (lokale Administration) nach einer Authentisierung durch Benutzername und Passwort (oder einen gleich starken oder stärkeren Authentisierungsmechanismus).

Application Note 17: **Vollständigkeit der Dienste:** Die Liste der im Folgenden genannten Dienste ist in dem Sinne vollständig, dass man sich weitere Dienste zwar vorstellen könnte, solche Dienste aber in diesem Schutzprofil bewusst nicht modelliert wurden.

- Beispielsweise erzwingt der VPN-Konzentrator die Nutzung des VPN-Tunnels (er leitet nur Pakete aus dem VPN-Tunnel zum Broker weiter). Der Netzkonnektor **unterstützt den VPN-Konzentrator** dabei, indem er das andere Ende des VPN-Tunnels implementiert. Dies stellt aber keine gesonderte Sicherheitsfunktionalität dar, sondern wird bereits unten unter Sicherheitsdienst (1) beschrieben.
- Eine **Vorabprüfung der Datensätze auf Plausibilität** (z.B. XML-Validierung) wird durch den Anwendungskonnektor vorgenommen; dies stellt für den Netzkonnektor keine Sicherheitsfunktionalität dar.
- Eine hohe **Verfügbarkeit des Konnektors** ist natürlich ein wichtiges Ziel im elektronischen Gesundheitswesen. Bei Nutzung von Infrastrukturen wie z.B. dem Internet kann eine bestimmte Verfügbarkeit jedoch nicht garantiert werden, weil diese von vielen nicht beeinflussbaren Einzelheiten abhängig ist. Daher wurde in diesem Schutzprofil darauf verzichtet, die Verfügbarkeit als Sicherheitsziel (siehe Abschnitt 4.1) zu formalisieren. Gleiches gilt sinngemäß für Quality of Service. Siehe auch Abschnitt 7.6.8.
- Dienste im Zusammenhang mit Fachlogik werden durch den Anwendungskonnektor erbracht, der nicht Gegenstand dieses Schutzprofils ist.
- Es wird angenommen, dass in eKiosken[16] auch Netzkonnektoren zum Einsatz kommen werden, dass sich aus diesem Einsatz heraus aber keine zusätzlichen Anforderungen an den Netzkonnektor ergeben.

Application Note 18: Der Netzkonnektor muss keine Transaktionssicherheit gewährleisten. Soweit Transaktionssicherheit aus Sicherheitsgründen erforderlich ist, wird sie im Primärsystem, durch den Anwendungskonnektor und/oder in der zentralen Telematikinfrastruktur hergestellt.

[16] Der eKiosk ist ein Primärsystem zur Verwaltung von Anwendungen und Daten durch den Versicherten. Mit Hilfe des eKiosk kann der Versicherte z.B. eRezepte ausblenden, das Einverständnis zum Laden diverser Anwendungen erklären usw.

Der EVG erbringt folgende Sicherheitsdienste:

(1) VPN-Client: Der EVG stellt dem Anwendungskonnektor (und damit mittelbar auch den Primärsystemen) einen sicheren Kanal (virtual private network, VPN) zur zentralen Telematikinfrastruktur zwecks Nutzung von zentralen Diensten bereit.

Application Note 19: Es kann weitere VPN-Kanäle für Mehrwertdienste (zu *VPN-Konzentratoren für Mehrwertdienste*, vgl. Application Note 22:) geben. Diese sind jedoch von dem hier geforderten streng getrennt. Außerdem werden VPN-Kanäle für Mehrwertdienste den Primärsystemen direkt angeboten, während der VPN-Kanal in die Telematikinfrastruktur zu den Diensten nach § 291 a SGB V ausschließlich über den Anwendungskonnektor erreicht werden kann (siehe auch unten, Punkt (c): regelbasierte Informationsflusskontrolle). Siehe auch die folgenden Sicherheitsdienste (2) (a) und (2) (b). Wenn in diesem Schutzprofil keine näheren Angaben gemacht werden, ist mit den Begriffen „VPN-Kanal“ oder „VPN-Tunnel“ stets der sichere Kanal zur zentralen Telematikinfrastruktur für Dienste gemäß § 291 a SGB V gemeint. Der ST-Autor soll erklären, ob und ggf. welche Mehrwertdienste der EVG unterstützt. Falls Mehrwertdienste unterstützt werden, soll der ST-Autor eine eindeutige Terminologie verwenden, so dass im Security Target stets eindeutig klar ist, welche VPN-Kanäle der EVG für welche Zwecke nutzt.

(a) Der EVG führt eine gegenseitige Authentisierung der Endpunkte (VPN-Client und VPN-Konzentrator) durch; diese erfolgt auf der Basis von IPsec und mit Hilfe von Zertifikaten nach dem Standard X.509v3. Siehe auch Sicherheitsdienst (3) (b) Gültigkeitsprüfung von Zertifikaten.

Der Netzkonnektor authentisiert sich gegenüber dem VPN-Konzentrator mittels Schlüsselmaterial, das sich auf einem Sicherheitsmodul SM-K (Sicherheitsmodul für den Netzkonnektor) befindet.

Aspekt	**Einheit, welche die Authentisierung ausführt**	
	Netz konnektor	**Anwendungs-konnektor**
Sicherheitsmodul, welches die kryptographische Identität speichert	SM-K	SMC-B
Identität, die durch das Sicherheits-modul repräsentiert wird	Netzkonnektor (bzw. seine Bauartzulassung)	Organisation des Leistungserbringers
Standard, in dem die kryptographische Identität vorgehalten wird	X.509-Zertifikat	X.509-Zertifikat
Gegenstelle, gegen welche die Authentisierung erfolgt	VPN-Konzentrator	Message Broker
Protokoll	IPsec (IP Security)	TLS (Transport Layer Security)

Tabelle 1: Authentisierungsschritte

(b) Die Nutzdaten, die über das VPN übertragen werden, werden hinsichtlich ihrer Vertraulichkeit und Datenintegrität geschützt (Verschlüsselung und Integritätsschutz[17] der Daten vor dem Versenden bzw. Entschlüsselung und Integritätsprüfung nach dem Empfangen). Dazu wird für die VPN-Verbindung ein Sitzungsschlüssel vereinbart. Der EVG verfügt über eine für den Benutzer leicht zugängliche Anzeige, die ihm die Betriebsbereitschaft sowie das Bestehen oder Nichtbestehen einer sicheren VPN-Verbindung zur zentralen Telematikinfrastruktur signalisiert.

(c) Der EVG setzt auch eine regelbasierte Informationsflusskontrolle um, d.h., regelbasiert müssen alle Informationsflüsse den etablierten VPN-Tunnel nutzen. Siehe auch Sicherheitsdienst (2) (b) Separationsmechanismen für Mehrwertdienste.

Der Netzkonnektor muss die Benutzung des VPN-Tunnels für den Versand von sensitiven Daten erzwingen bzw. ungeschützten Zugriff auf das Transportnetz verbieten. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer *zu schützende Daten* absichtlich preisgibt[18], aber er muss ihre versehentliche Preisgabe verhindern. Dazu wird angenommen, dass sensitive Daten vom Anwendungskonnektor erkannt werden und dem Netzkonnektor als sensitiv gekennzeichnet[19] übergeben werden (siehe A.AK).

(2) Dynamischer Paketfilter (mit zustandsgesteuerter Filterung): Der EVG bindet die Primärsysteme sicher an die Telematikinfrastruktur an.

(a) Dazu verfügt der EVG über die Funktionalität eines dynamischen Paketfilters, welcher entsprechende Regeln umsetzen kann. Er schränkt die Menge der zulässigen Protokolle ein. Der EVG schützt sich selbst und das lokale Netz des Leistungserbringers vor Angriffen aus dem Transportnetz und dem lokalen Netz des Leistungserbringers; hierbei werden Angriffe mit hohem Angriffspotential abgewehrt. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz geeignet zum Schutz der Primärsysteme.

Application Note 20: Bei der Betrachtung von Angriffen aus dem LAN sind auch solche Bedrohungsszenarien zu berücksichtigen, bei denen auf anderen Wegen (z.B. Wechseldatenträger wie CD, DVD, USB-Stick, Diskette) Schadsoftware in die IT-Systeme im LAN des Leistungserbringers kommen kann. Ein **LAN-seitiger Paketfilter** hindert solche Schadsoftware daran,

- die Integrität des Konnektors zu bedrohen,
- über das VPN auf die zentrale Telematikinfrastruktur zuzugreifen, oder

[17] Message Authentication Code bzw. HMAC

[18] Beispielsweise könnte ein Leistungserbringer *zu schützende Daten* von einem Primärsystem aus lokal auf Wechseldatenträger kopieren oder im Rahmen eines Mehrwertdienstes als verschlüsselten E-Mail-Anhang (und damit für den Konnektor nicht erkennbar) versenden.

[19] Die „Kennzeichnung“ wird dabei technisch umgesetzt durch den Aufruf geeigneter Schnittstellen des Netzkonnektors.

- über das Internet Kontakt mit der Außenwelt aufzunehmen und unbemerkt z.B. sensitive Daten zu verschicken oder weitere Schadsoftware nachzuladen.

Ferner sind auch Szenarien denkbar, in denen durch Paketfilterung kein vollständiger Schutz erreicht werden kann. Die BSI Firewall Studie II [57] empfiehlt daher in ihrem Abschnitt 4.1 mit Verweis auf „*Firewalls and Internet Security*“ [58] den Einsatz eines von LAN- und WAN-seitigen Paketfiltern umgebenen Applikationsfilters (Application Layer Gateway, häufig auch als Proxy bezeichnet).

Die Inhalte der Kommunikation über den oder die VPN-Tunnel für Mehrwertdienste werden vom Konnektor nicht ausgewertet. Siehe auch den folgenden Sicherheitsdienst (2) (b).

Siehe auch Abschnitt 7.6.6.

Application Note 21: Der Netzkonnektor muss kein **Application Layer Gateway** enthalten. Der Anwendungskonnektor übernimmt in weiten Teilen die Aufgaben eines solchen Application Layer Gateways. Der Anwendungskonnektor wird topologisch von beiden Seiten von einem Paketfilter umgeben (LAN-seitig und WAN-seitig, d.h. gegenüber dem Primärsystemnetz und gegenüber dem Transportnetz).

(b) Der Konnektor bietet Separationsmechanismen für Mehrwertdienste, d.h., er schützt die evaluierte Sicherheitsfunktionalität und die Verarbeitung der medizinischen Daten vor möglicherweise schädlichem Einfluss von Mehrwertdiensten. Siehe auch Sicherheitsdienst (1) (c) regelbasierte Informationsflusskontrolle. Es wird grundsätzlich jeder nicht vom Anwendungskonnektor generierte, direkte Verkehr aus dem LAN in den VPN-Tunnel für Dienste gemäß § 291 a SGB V ausgeschlossen (mit Ausnahme des VPN-Verbindungsaufbaus, der nicht durch den VPN-Tunnel läuft, aber für den Aufbau des Tunnels erforderlich ist). Optional kann weiterer Verkehr in Richtung WAN über einen oder mehrere weitere VPN-Tunnel für Mehrwertdienste geleitet werden; diese weiteren VPN-Tunnel werden durch den Netzkonnektor streng vom VPN-Tunnel für Dienste gemäß § 291 a SGB V separiert. Die Inhalte der Kommunikation über den oder die VPN-Tunnel für Mehrwertdienste werden vom Konnektor nicht ausgewertet. In jedem Fall (auch bei Nutzung von Mehrwertdiensten) unterbindet der Netzkonnektor direkte Kommunikation (außerhalb von VPN-Kanälen) ins Transportnetz (Internet) mit Ausnahme der für den VPN-Verbindungsaufbau erforderlichen Kommunikation.

Application Note 22: Siehe auch Abschnitt 7.6.15.

(c) Der Netzkonnektor bietet grundlegende Intrusion Prevention-Funktionalität: Er kann nicht wohlgeformte IP-Pakete erkennen. Der EVG implementiert eine zustandsgesteuerte Filterung (stateful packet inspection[20]).

[20] stateful packet inspection: dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird; der Verbindungsstatus eines Datenpakets wird in die Entscheidung einbezogen, ob ein Informationsfluss zulässig ist oder nicht

Application Note 23: Der Konnektor soll kein netzwerkbasiertes Intrusion Detection System (IDS) für das Primärsystemnetz realisieren, sondern sich auf grundlegende Intrusion Prevention-Funktionalität beschränken. Er generiert aber im Rahmen der zustandsgesteuerten Filterung (zumindest temporär) **Audit-Daten**, siehe FAU_GEN.1/Stateful. Diese Audit-Daten dürfen weder mit dem Ereignisprotokoll (siehe FAU_GEN.1/Audit) noch mit der vom Anwendungskonnektor gesteuerten Protokollierung von medizinischen Daten (auf der eGK oder in der zentralen Telematikinfrastruktur) verwechselt werden: Der Konnektor speichert keine medizinischen Daten dauerhaft. Die von FAU_GEN.1/Stateful erzeugten Audit-Daten (Log-Daten) dienen lediglich dem Netzkonnektor selbst sowie gegebenenfalls einem Administrator dazu, eine dynamische bzw. zustandsgesteuerte Paketfilterung durchzuführen – sie stellen den Zustand (engl. *state*) der stateful packet inspection dar. Gegebenenfalls können die von FAU_GEN.1/Audit erzeugten Audit-Daten dabei ebenfalls hilfreich sein; es wird jedoch nicht gefordert, dass der EVG die von FAU_GEN.1/Audit erzeugten Audit-Daten selbst auswertet. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

(3) Netzdienste: Der EVG bietet folgende netzbasierte Dienste an:

(a) Echtzeituhr/Zeitsynchronisation: Der EVG verfügt über eine Echtzeituhr mit einer zu spezifizierenden Freilaufgenauigkeit und führt in regelmäßigen Abständen eine Zeitsynchronisation mit einem zentralen Zeitdienst durch.

Die vom EVG bereitgestellte Zeit-Information wird wie folgt genutzt, um Informationen mit einem Zeitstempel zu versehen:

- Der Netzkonnektor generiert Audit-Daten zur späteren Auswertung mit dem Ziel Intrusion Prevention (zustandsgesteuerte Filterung).

Application Note 24: Dabei hängt die Qualität und Beweiskraft solcher Zeitstempel von der Qualität der Echtzeituhr und von weiteren Bedingungen ab.

Optional kann der Netzkonnektor die Zeit-Information für weitere Zwecke verwenden oder auch anderen dezentralen Komponenten zur Verfügung stellen. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet. – Siehe auch Spezifikation Infrastrukturkomponenten: Zeitdienst [30].

Application Note 25: Der ST-Autor kann optional Maßnahmen zur **Sicherung des Kommunikationskanals** zwischen dem Netzkonnektor und dem zentralen Zeitdienst fordern, sofern dies von der zentralen Infrastruktur unterstützt wird. Als Maßnahmen kommen insbesondere in Frage: (a) Integritätsschutz der übertragenen Zeit und (b) vorherige Authentisierung des zentralen Zeitdienstes gegenüber dem Netzkonnektor. Mindestens gefordert ist eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_TDC.1/Time. Siehe dazu Spezifikation Infrastrukturkomponenten: Zeitdienst [30], Abschnitt 5.1.1.6 (Realisierbarkeit des Autokey-Sicherheitsmodells wird gegenwärtig geprüft) sowie Abschnitt 6.1. Zu beachten ist, dass die Konnektor-Spezifikation [20] vorsieht, dass die Zeitsynchronisation ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur erfolgt, d.h. über *VPN-Konzentratoren für Dienste gemäß § 291 a SGB V*. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet. Die Funktionalität soll sich dabei an den aktuellen Versionen der Konnektor-Spezifikation [20] orientieren.

(b) Gültigkeitsprüfung von Zertifikaten: Der EVG muss die Gültigkeit von Zertifikaten überprüfen, die für den Aufbau des VPN-Kanals verwendet werden. Die Zertifikate werden mathematisch und gegen Sperrlisten geprüft. Siehe auch Sicherheitsdienst (1) (a) gegenseitige Authentisierung.

(4) Stateful Packet Inspection: Der EVG generiert Audit-Daten für eine spätere Auswertung mit dem Ziel Intrusion Prevention (zustandsgesteuerte Filterung).

Application Note 26: Eine über die grundlegende Intrusion Prevention hinausgehende Auswertung der Audit-Daten kann optional außerhalb des EVG (in seiner IT-Einsatzumgebung) erfolgen. In diesem Fall soll der ST-Autor FAU_SAR.1/Env geeignet anpassen (um FAU_GEN.1/Stateful erweitern).

(5) Selbstschutz: Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren.

(a) Speicheraufbereitung: Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben. Der EVG speichert medizinische Daten nicht dauerhaft und löscht sie sobald wie möglich durch aktives Überschreiben.

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

Application Note 27: Optional kann der EVG weitergehende Mechanismen zum Selbstschutz implementieren, beispielsweise **physische Sicherheitsmaßnahmen** (Erkennung von bzw. Reaktion auf Angriffe auf das Gehäuse). Der ST-Autor kann solche Anforderungen als Differenzierungsmerkmal in das Security Target aufnehmen. Siehe auch Application Note 4: *Möglichkeit zur Differenzierung* und Abschnitt 7.6.7.

Application Note 28: Der EVG kann für die Integritätsprüfung einen externen Vertrauensanker verwenden, um die Unversehrtheit des EVGs zu überprüfen. Dies gilt insbesondere im Fall reiner Software-Lösungen. Beispielsweise könnte ein externes Prüfprogramm auf einem nicht wiederbeschreibbaren Datenträger (z.B. CD-ROM) einen authentischen public key als Signaturprüfschlüssel verwenden, um Hashwerte bzw. Signaturen der installierten Programmdateien und –bibliotheken zu überprüfen. Siehe auch Application Note 2: Mechanismen zum Integritätsschutz.

Alternativ muss der EVG den Vertrauensanker in seinem sicheren Schlüsselspeicher aufbewahren (siehe Sicherheitsdienst (5) (c)). Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

(c) Der EVG bietet einen sicheren Schlüsselspeicher.

Eine Auflistung der Schlüssel, die im sicheren Schlüsselspeicher gespeichert werden, findet sich unter der Zwischenüberschrift „Sicherer Schlüsselspeicher“ in Abschnitt 5.1.1.5.

Die Konnektor-Spezifikation [20], Version 2.0.0, listet in Abschnitt 4.2.1 Anforderungen an die Speicherung von Schlüsselmaterial im SM-K auf. Dieser

Schlüsselspeicher wird durch das SM-K (in der IT-Einsatzumgebung) implementiert (siehe OE.SM-K). Darüber hinaus muss der EVG über einen weiteren sicheren Schlüsselspeicher für die in Abschnitt 5.1.1.5 aufgelisteten Schlüssel verfügen.

Application Note 29: Optional (als Differenzierungsmerkmal) kann gefordert werden, dass der sichere Schlüsselspeicher physischen Angriffen widersteht. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

(d) Der EVG schützt Geheimnisse (insbesondere Schlüssel) während ihrer Verarbeitung gegen unbefugte Kenntnisnahme.

(e) (optional) Der EVG kann sichere Kanäle zu anderen vertrauenswürdigen dezentralen Komponenten etablieren.

Application Note 30: Abhängig von der Ausgestaltung des Konnektors ist ein sicherer Kanal zwischen Netzkonnektor und Anwendungskonnektor zu etablieren. Die Forderung nach einem sicheren Kanal zwischen Netzkonnektor und Anwendungskonnektor kann bei einer Einbox-Lösung entfallen (siehe auch Application Note 6: Einbox- vs. Mehrbox-Lösung). Siehe auch Abschnitt 7.6.16.

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

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

Der ST-Autor soll in konsistenter Weise beschreiben, welchen Bedrohungen die Verbindungen zwischen Anwendungskonnektor, Netzkonnektor und SM-K ausgesetzt sind, welche Annahmen an die Einsatzumgebung gelten und welche Funktionalität genau der EVG im Hinblick auf sichere Kanäle bietet. – Siehe auch Abschnitt 7.6.16.

(f) Protokollierung: Der EVG führt ein Ereignisprotokoll (Sicherheits-Log, Security Log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Ereignisprotokoll reservierte Speicher muss hinreichend groß dimensioniert sein. Der EVG protokolliert die folgenden Ereignisse (vgl. auch Konnektor-Spezifikation [20], Version 2.0.0, Abschnitt 4.2.3.2, Nicht-funktionale Anforderungen an den Betrieb des Konnektors, Protokollierung):

- Ein- und Ausschalten (power on, shut down, reset),
- Aufbau und Abbruch der VPN-Verbindung sowie VPN-Fehler,
- Identität der VPN-Konzentratoren, mit denen der EVG eine Verbindung aufgebaut hat sowie
- Software-Updates und
- Zeitpunkt und Art der Änderungen von Konfigurationseinstellungen.

Application Note 31: Der ST-Autor soll diese Liste der zu protokollierenden Ereignisse mit der jeweils aktuellen Version der Konnektor-Spezifikation [20] abgleichen und auch die funktionale Anforderung FAU_GEN.1/Audit geeignet anpassen. Siehe auch Application Note 99:.

Application Note 32: Die Auswertung des Ereignisprotokolls kann sowohl durch den EVG als auch durch die Einsatzumgebung erfolgen; dieses Schutzprofil formuliert daher den Fall, dass die Auswertung durch die Einsatzumgebung erfolgt (siehe FAU_SAR.1/Env in Abschnitt 5.2.3). Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

Das Ereignisprotokoll muss Aktivitäten des Administrators manipulationsfrei aufzeichnen, somit darf der Administrator das Ereignisprotokoll nicht löschen können. Wenn der für die Audit-Daten reservierte Speicherbereich aufgebraucht ist, muss der EVG diesen zyklisch überschreiben.

Application Note 33: Hinweis: Ein unbeaufsichtigtes zyklisches Überschreiben der Audit-Daten birgt die Gefahr, dass ein Angreifer unerwünschte Audit-Daten durch neuere, harmlose Daten überschreiben kann. In diesem Schutzprofil wird daher davon ausgegangen, dass der für das Sicherheits-Log vorgesehene Speicherbereich hinreichend groß ist, so dass diese Gefährdung üblicherweise nicht zutreffend ist, und dass ferner absichtlich herbeigeführte Einträge im Sicherheits-Log bei der Log-Auswertung als solche erkannt werden können. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet, so dass diesen Annahmen (hinreichend großer Speicher für Audit-Daten, Erkennbarkeit von absichtlich herbeigeführten Einträgen) gerechtfertigt werden können.

(6) Administration

(a) Der EVG erlaubt eine gesicherte Aktualisierung der Firmware und Software des Konnektors (Sicheres Update). Dies umfasst einen sicheren Download von Updates und deren automatische Integritätsprüfung und Aktivierung sowie eine Sequenzkontrolle (Aktivierung der neuen Software erst nach erfolgreicher Integritätsprüfung und erfolgreicher Installation) und die Wiederherstellung eines sicheren Zustands, falls es im Rahmen des Update-Prozesses zu Fehlern kommen sollte.

Application Note 34: Der ST-Autor soll spezifizieren, welche Teile des Konnektors aktualisiert werden können sollen. Beispiele sind: Firmware, Software (Betriebssystem-Software, Anwendungssoftware) und Regelsätze für die Paketfilter. Das Security Target soll beschreiben, auf welche Weise sichergestellt wird, dass nur authentische Teile aktiviert werden können. Der Netzkonnektor kann beispielsweise über einen unveränderlichen Boot-Loader verfügen, welcher die Integrität der nachzuladenden Teile sicherstellt. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

(b) Der EVG bietet eine lokale Managementschnittstelle an.

Application Note 35: Es soll möglich sein, Wartungsaktivitäten (einschließlich Monitoring und Konfiguration) durchzuführen, ohne den zertifizierten Status des Netzkonnektors zu verlieren (dabei wird davon ausgegangen, dass bei der Wartung die Benutzer- und Administratordokumentation des EVG beachtet wird). Abhängig von der Mächtigkeit der Wartungsschnittstelle sind spezifische Separationsmechanismen erforderlich (z.B. aus der Familie FPT_SEP), welche sicherstellen, dass die Sicherheitsfunktionalitäten des EVG durch die Wartung nicht beeinträchtigt werden. Der ST-Autor kann auch eine Verfeinerung der Komponenten AGD_ADM.1 und/oder AVA_MSU.3 in Betracht ziehen.

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

Eine Möglichkeit zur Fernwartung ist wünschenswert, wird aber nicht verpflichtend gefordert. Falls eine Möglichkeit zur Fernwartung vorhanden ist, muss diese hinreichend gut abgesichert werden. Zur Absicherung der Fernwartung können dieselben oder ähnliche Mechanismen verwendet werden wie zur Absicherung der lokalen Administration an der LAN-Schnittstelle (z.B. sicherer TLS-Kanal zwischen Administrator-Arbeitsplatz und Netzkonnektor wie bei FTP_TRP.1/Admin, Authentisierung des Administrators wie bei FIA_UAU.1/SMR).

(c) Der EVG erzwingt eine sichere Authentisierung des Administrators vor administrativen Aktivitäten. Nur authentisierte Administratoren dürfen administrative Tätigkeiten und Wartungsarbeiten durchführen.

Application Note 36: Die **Authentisierung des Administrators** muss verhindern, dass Unbefugte administrative Tätigkeiten vornehmen. Der EVG muss eine Authentisierungsfunktion bieten (z.B. Passwort-Prüfung). Hersteller können ihre Produkte durch die unterstützen Formen der Authentisierung differenzieren. Die Authentisierung der Administratoren muss mindestens durch eine Authentisierung mittels Wissen erfolgen. Optional kann die Authentisierung auch durch Besitz und Wissen geschützt werden. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

3. Definition des Sicherheitsproblems (EVG-Sicherheitsumgebung)

In diesem Abschnitt wird zunächst beschrieben, welche Werte der EVG schützen muss, welche Subjekte 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.

3.1. Zu schützende Werte

Werte sind durch Gegenmaßnahmen zu schützende Informationen oder Ressourcen. Der Schutz kann durch den EVG oder durch die Umgebung erfolgen; diese Aufteilung erfolgt in Kapitel 4.

Zu schützende Daten

Der Begriff „*zu schützende Daten*“ bezeichnet im Folgenden stets medizinische oder sonstige personenbezogene Daten, die vor dem Zugriff durch Unbefugte/Angreifer zu schützen sind. Diese Daten sind User Data im Sinne der Common Criteria. Sie umfassen bei den Pflichtanwendungen mindestens die Versichertenstammdaten[21] und Verordnungen (eRezepte) sowie sonstige Daten, die im Rahmen der Abwicklung dieser Pflichtanwendungen entstehen (etwa Dispensierdaten).

Application Note 37: Bei der Nutzung freiwilliger Anwendungen nach § 291 a SGB V (z.B. elektronische Patientenakte, elektronischer Arztbrief, etc.) ist diese Definition sinngemäß zu erweitern.

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

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

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

3.1.1. Primäre Werte

Die primären Werte sind in der folgenden Tabelle 2 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur (beide Übertragungsrichtungen)	Vertraulichkeit, Integrität, Authentizität	Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur werden *zu schützende Daten* ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein. ⇒ T.remote_VPN_Data, A.AK
zu schützende Daten im Primärsystem	Vertraulichkeit, Integrität	Auf den Primärsystemen werden *zu schützende Daten* vorgehalten. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten manipulieren können. ⇒ T.remote_TOE_LAN, T.local_TOE_LAN, A.phys_Schutz
in der zentralen Telematikinfrastruktur oder auf Chipkarten gespeicherte *zu schützende Daten*	Vertraulichkeit, Integrität	Werden *zu schützende Daten* in der zentralen Telematikinfrastruktur gespeichert, so müssen 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*, die auf Chipkarten abgelegt werden. ⇒ T.remote_VPN_Data, A.sichere_TI
Primärsystem, Anwendungskonnektor	Integrität	Manipulierte Primärsysteme oder Anwendungskonnektoren können dazu führen, dass *zu schützende Daten* abfließen oder unautorisiert verändert werden. Im normalen Betrieb wird davon ausgegangen, dass *zu schützende Daten* das Primärsystem nur dann verlassen, wenn sie in die zentrale Telematikinfrastruktur oder auf eine eGK übertragen werden sollen. Daher werden *zu schützende Daten* nur an den Anwendungskonnektor übermittelt. Ein manipuliertes Primärsystem könnte Kopien der Daten einem Angreifer zugänglich machen oder auch *zu schützende Daten* gezielt verändern. Ein manipulierter

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		Anwendungskonnektor könnte *zu schützende Daten* falsch „kennzeichnen“[22] und so die korrekte Übermittlung durch den Netzkonnektor (über den VPN-Kanal für Dienste gemäß § 291 a SGB V) verhindern. Auf diese Weise könnte einem Versicherten oder einem Leistungserbringer Schaden zugefügt werden. ⇒ T.remote_TOE_LAN, A.Betrieb_AK, A.phys_Schutz
Systeme der zentralen Telematik-infrastruktur	Verfügbarkeit	Der Anwendungskonnektor kann Syntaxprüfungen und Plausibilisierungen von Anfragen an die zentrale Telematikinfrastruktur durchführen und auf diese Weise dazu beitragen, dass weniger nicht wohlgeformte Anfragen an die zentrale Telematikinfrastruktur gerichtet werden. Bei diesen Aspekten handelt es sich aber um Bedrohungen der zentralen Telematikinfrastruktur und nicht um Bedrohungen des EVG. Außerdem kann der Konnektor nicht für die Verfügbarkeit von Diensten garantieren; daher wird Verfügbarkeit nicht als Sicherheitsziel für den EVG formuliert. Siehe auch Abschnitt 7.6.8 und Abschnitt 3.4.2.4, Stichwort *komplementäre Bedrohung*. ⇒ A.kein_DoS, A.Ersatzverfahren Siehe auch Abschnitt 7.6.8 und Application Note 17:.

Tabelle 2: Primäre Werte

3.1.2. Sekundäre Werte

Die sekundären Werte sind in der folgenden Tabelle 3 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten im EVG	Vertraulichkeit,	Auch während der Verarbeitung im EVG müssen *zu schützende Daten* gegen unbefugte

[22] Die „Kennzeichnung“ erfolgt technisch durch die Übergabe der Daten vom AK an eine definierte Schnittstelle des NK.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
	Integrität	Kenntnisnahme und Veränderung geschützt werden. ⇒ T.local_TOE_LAN, T.remote_TOE_WAN,
EVG	Integrität	Gelingt es einem Angreifer, die Integrität des EVG zu verletzen, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Es ist zu befürchten, dass dann *zu schützende Daten* unbefugt zur Kenntnis genommen oder unbemerkt manipuliert werden können. ⇒ alle Bedrohungen, gegen die O.Schutz wirkt (T.local_TOE_LAN, T.remote_TOE_WAN, T.remote_TOE_LAN, T.local_admin_LAN, T.remote_admin_WAN) sowie T.counterfeit
EVG-Updates	Integrität, Authentizität	Falls der EVG ein sicheres Update unterstützt, muss er Integrität und Authentizität der Software vor ihrer Aktivierung überprüfen. Andernfalls ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ T.local_admin_LAN, T.remote_admin_WAN
kryptographisches Schlüsselmaterial (während seiner Speicherung im EVG oder Verwendung durch den EVG)	Vertraulichkeit, Integrität, Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikations-partners sicherzustellen. ⇒ A.phys_Schutz, alle Bedrohungen, gegen die O.Schutz und O.VPN_Auth wirken (T.local_TOE_LAN, T.remote_TOE_WAN, T.remote_TOE_LAN, T.remote_VPN_Data, T.local_admin_LAN, T.remote_admin_WAN) sowie T.Zert_Prüf
Administrative Funktionalitäten des EVG	Zugriffsschutz	Nur autorisierte Administratoren dürfen den EVG administrieren. ⇒ T.local_admin_LAN, T.remote_admin_WAN, A.Admin_EVG
Authentisierungs-geheimnisse (im EVG gespeicherte	Vertraulichkeit	Die Vertraulichkeit von Authentisierungs-geheimnissen (z.B. Passwort für Administrator-authentisierung, evtl. PIN für die SM-K) ist zu

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
Referenzdaten und zum EVG übertragene Verifikationsdaten)		schützen. ⇒ A.phys_Schutz, alle Bedrohungen, gegen die O.Schutz wirkt (T.local_TOE_LAN, T.remote_TOE_WAN, T.remote_TOE_LAN, T.local_admin_LAN, T.remote_admin_WAN)
Management-Daten (während ihrer Übertragung zum EVG)	Vertraulichkeit, Integrität und Authentizität	Wenn der EVG administriert wird, dürfen die administrativen Datenströme nicht eingesehen oder unbemerkt verändert werden können. ⇒ alle Bedrohungen, gegen die O.Admin_EVG und OE.Admin_EVG wirken, insbesondere T.local_admin_LAN und T.remote_admin_WAN
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.phys_Schutz, alle Bedrohungen, gegen die O.Schutz wirkt (T.local_TOE_LAN, T.remote_TOE_WAN, T.remote_TOE_LAN, T.local_admin_LAN, T.remote_admin_WAN)
Audit-Daten (Security Log)	Existenz, Integrität, Verfügbarkeit	Der EVG muss Audit-Daten generieren, anhand derer Veränderungen an der Konfiguration des EVG nachvollzogen werden können (vgl. O.Protokoll und FAU_GEN.1/Audit). Niemand darf Audit-Daten löschen oder verändern können. Wenn der für die Audit-Daten vorgesehene Speicherbereich aufgebraucht ist, müssen die Audit-Daten zyklisch überschrieben werden. Die Audit-Daten müssen auch zum Nachweis der Aktivitäten von Administratoren verwendet werden können. Der EVG erzeugt Audit-Daten (den „Zustand“ für die zustandsgesteuerte Filterung) über die Aktivitäten der Paketfilter für eine Auswertung mit dem Ziel Intrusion Prevention (zustandsgesteuerte Filterung), vgl. O.Stateful und FAU_GEN.1/Stateful. ⇒ alle Bedrohungen, gegen die O.Protokoll und O.Stateful wirken (T.remote_TOE_WAN sowie möglicherweise viele andere auch, abhängig vom

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		Umfang der Protokollierung, siehe auch Application Note 57:)
Zeit	Existenz, Gültigkeit	Der EVG muss eine gültige Systemzeit vorhalten und diese regelmäßig mit einem Zeitserver synchronisieren. Die Zeit wird für die Prüfung der Gültigkeit von VPN-Zertifikaten sowie für die Erzeugung von Zeitstempeln in Audit-Daten (Log-Daten) verwendet. ⇒ T.TimeSync, alle Bedrohungen, gegen die O.Zeit wirkt (T.remote_TOE_WAN, T.remote_TOE_LAN, T.remote_VPN_Data)

Tabelle 3: Sekundäre Werte

Application Note 38: Im Falle von Mehrbox-Lösungen sind als sekundäre Werte auch die zwischen den Boxen ausgetauschten Nachrichten zu betrachten. Beispiel:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung
Nachrichten zwischen Konnektorteilen (Boxen), welche *zu schützende Daten* enthalten	Integrität	Verfälschung von *zu schützenden Daten*
	Authentizität	Verfälschung des Absenders, Replay-Angriff
	Vertraulichkeit	Abfluss *zu schützender Daten*
Nachrichten zwischen Konnektorteilen (Boxen), welche Schlüsselmaterial enthalten	Integrität	Verfälschung von Schlüsseln (etwa mit der Folge, dass ein „sicherer Kanal“ unsicher wird)
	Authentizität	Verfälschung des Absenders, Replay-Angriff
	Vertraulichkeit	Abfluss von Schlüsselmaterial

3.2. Akteure und ihr Interesse am Netzkonnektor

Eine Auflistung der in die Prozesse rund um den Netzkonnektor involvierten Akteure findet sich in der Konnektor-Spezifikation [20], Version 2.0.0, Abschnitt 3.6.2.1 *Akteure*.

3.3. Subjekte und Objekte

Die Formulierung des Sicherheitsproblems (Security Problem Definition) erfolgt unter Verwendung der im Folgenden beschriebenen Subjekte und Objekte.

3.3.1. Subjekte

Es werden die folgenden Subjekte[23] betrachtet:

NK Netzkonnektor (engl.: network connector; the TOE),

AK Anwendungskonnektor (engl.: application connector),

VPN-K entfernter VPN-Konzentrator (engl.: VPN concentrator), der den Zugriff auf die Telematikinfrastruktur vermittelt,

PS Primärsystem (engl.: workstation),

NK-Admin oder auch **NK-Administrator** (NK administrator): Administrator des Netzkonnektors,

Angreifer ein Angreifer (engl.: attacker).

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

Der Angreifer kann sich sowohl

- gegenüber dem Netzkonnektor als (gefälschter) VPN-Konzentrator als auch
- gegenüber dem VPN-Konzentrator als (gefälschter) Netzkonnektor ausgeben.

Ersteres wird durch die Bedrohungen T.remote_TOE_WAN, T.remote_TOE_LAN, T.remote_VPN_Data und T.remote_admin_WAN abgebildet. Letzteres stellt eine Bedrohung des VPN-Konzentrators dar und ist daher nur indirekt Gegenstand der Betrachtung (siehe auch O.VPN_Auth: EVG muss eine gegenseitige Authentisierung durchführen).

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.

[23] Definitionen in Common Criteria [1], Kapitel 3: ***subject*** *:= an entity within the TSC (TOE scope of control) that causes operations to be performed;* ***object*** *:= an entity within the TSC that contains or receives information and upon which subjects perform operations.*

Für den **Leistungserbringer** sind die Leistungen des NK transparent, er arbeitet mit dem Primärsystem. Sofern er Einstellungen des NK verändert, agiert er in der Rolle des NK-Admin. Deshalb ist der Leistungserbringer nicht gesondert als eigenes Subjekt modelliert. Auch ein Leistungserbringer kann in der Rolle des Angreifers auftreten: Innerhalb des NK gibt es Geheimnisse (z.B. Sitzungsschlüssel des VPN-Kanals oder eventuelle geheime oder private Schlüssel zur Entschlüsselung von Software-Updates), die auch der 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 Primärsysteme 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.phys_Schutz sicherstellen muss.

3.3.2. Objekte

Es werden die folgenden Objekte[23] betrachtet:

PS-Daten lokal beim Leistungserbringer (in Primärsystemen im LAN) gespeicherte *zu schützende Daten*,

VPN-Daten *zu schützende Daten* während des Transports zwischen NK und VPN-K,

TI-Daten entfernt in den Datenbanken der Telematikinfrastruktur gespeicherte *zu schützende Daten*.

Es wird davon ausgegangen, dass die VPN-Daten durch den zwischen NK und VPN-K implementierten sicheren Kanal (d.h. durch das VPN) geschützt werden und dass die TI-Daten entweder nur in verschlüsselter Form gespeichert vorliegen (z.B. eRezept) oder dass Angriffe auf diese Daten durch organisatorische Maßnahmen abgewehrt werden (siehe A.sichere_TI in Abschnitt 3.6). Die Sicherheit der Primärsysteme ist nicht Gegenstand der Betrachtung.

3.4. Bedrohungen

3.4.1. Auswahl der betrachteten Bedrohungen

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

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

schon möglich. Der Netzkonnektor muss aber verhindern, dass Angreifer Zugriff auf Daten neuer Qualität oder neuer Quantität erhalten, etwa durch unbemerktes Mitlesen elektronischer Daten oder durch den Zugriff auf zentral gespeicherte Daten auf den Servern der zentralen 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)[24],
- 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 Facharzt 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 und Festnahme besteht.

Die Einführung der Telematikinfrastruktur ist durch folgende Eigenschaften gekennzeichnet:

- Daten liegen in elektronischer Form vor und werden so gespeichert.
- In der zentralen Telematikinfrastruktur werden große Datenmengen gespeichert und es werden Daten über einen Versicherten von verschiedenen Fachärzten aggregiert, so dass der Schutzbedarf der Daten aufgrund der größeren Datenmenge wachsen kann. Ferner werden auch über einen Leistungserbringer Daten aggregiert.
- Die Übertragung von Daten zwischen Leistungserbringer und zentraler Telematikinfrastruktur erfolgt unter Nutzung potentiell unsicherer Transportnetze.

Dies führt zu folgenden Angriffspunkten:

1. Die Vertraulichkeit oder Integrität von TI-Daten, die in der zentralen Telematik-infrastruktur gespeichert sind, wird bedroht. Dies kann physisch vor Ort oder logisch über Netzwerkverbindungen erfolgen. Dieser Angriff kann durch den Netzkonnektor nicht verhindert werden, sondern muss durch die VPN-Konzentratoren abgewehrt werden.

2. Die Vertraulichkeit oder Integrität von PS-Daten, die lokal beim Leistungserbringer gespeichert sind, wird bedroht. Hier ist insbesondere der Aspekt zu erwähnen, dass die IT-Systeme des Leistungserbringers üblicherweise an unsichere Transportnetze (z.B. Internet) angeschlossen werden und über diesen Weg Angriffe möglich werden. Der Netzkonnektor muss eine sichere Anbindung an die zentrale

[24] Allerdings verarbeiten auch schon vor der Einführung der elektronischen Gesundheitskarte viele Leistungserbringer Patientendaten elektronisch.

Telematikinfrastruktur bereitstellen und das lokale Netz des Leistungserbringers mit den Primärsystemen vor Angriffen aus dem Transportnetz schützen.

3. Die Vertraulichkeit oder Integrität von VPN-Daten, die zwischen dem lokalen Leistungserbringer und der zentralen Telematikinfrastruktur 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 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 PS-Daten, siehe T.remote_TOE_WAN und T.remote_TOE_LAN) sowie
- Angriffe aus dem Transportnetz auf die Datenübertragung zwischen dem lokalen Netz des Leistungserbringer und der zentralen Telematikinfrastruktur (mit Ziel VPN-Daten, siehe T.remote_VPN_Data); hier sind die Vertraulichkeit und Integrität der übertragenen Daten sowie die Authentizität von Sender und Empfänger bedroht.
- Lokale Angriffe auf die Integrität des Netzkonnektors (siehe T.local_TOE_LAN) mit dem Ziel, dessen Sicherheitseigenschaften zu schwächen oder zu verändern.
- Schließlich erlaubt der EVG lokale und optional auch entfernte Administration, die ebenfalls das Ziel von Angriffen sein kann (siehe T.local_admin_LAN und T.remote_admin_WAN).

3.4.2. Liste der Bedrohungen

Die folgende Abbildung 4 zeigt die beschriebenen Subjekte, Objekte und Angriffspfade (nummerierte Pfeile) im Zusammenhang.

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt, da es mehrere topologische Möglichkeiten der Anordnung des Anwendungskonnektors in Relation zum Netzkonnektor gibt (siehe auch Abbildung 2 und Abbildung 3 in Abschnitt 2.1). Das Kästchen „LAN-Interface“ stellt entweder die Verbindung zum Anwendungskonnektor dar oder schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

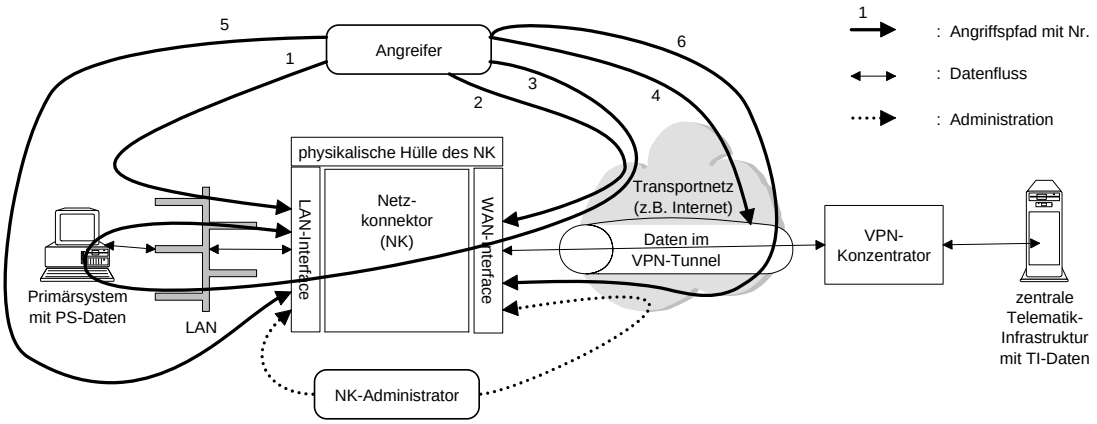

Abbildung 4: Subjekte und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 4 visualisierten Angriffspfaden (Nr. 1 bis Nr. 6) bzw. den zugeordneten Bedrohungen könnte ein Angreifer

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

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

Angriffspfad	Bezeichner	Beschreibung in Abschnitt
Nr. 1	T.local_TOE_LAN	3.4.2.1
Nr. 2	T.remote_TOE_WAN	3.4.2.2
Nr. 3	T.remote_TOE_LAN	3.4.2.3
Nr. 4	T.remote_VPN_Data	3.4.2.4
Nr. 5	T.local_admin_LAN	3.4.2.5
Nr. 6	T.remote_admin_WAN	3.4.2.6
Konnektornachbauten	T.counterfeit	3.4.2.7
Zertifikatsstatusabfragen	T.Zert_Prüf	3.4.2.8
Zeitsynchronisation	T.TimeSync	3.4.2.9

Tabelle 4: Kurzbezeichner der Bedrohungen

In den folgenden Abschnitten werden die Bedrohungen genauer beschrieben.

Die Angriffe, deren Bezeichner das Wort „local“ enthalten (T.local_TOE_LAN und T.local_admin_LAN) nehmen an, dass der Angreifer lokal in den Räumlichkeiten des Leistungserbringers agiert, setzen also einen unbefugten Zugriff auf den Netzkonnektor (z.B. Einbruch) voraus. Dabei wird angenommen, dass Personen, die berechtigten Zugang zu Räumlichkeiten des Leistungserbringers haben, entweder vertrauenswürdig[25] sind (so dass von ihnen keine Bedrohungen ausgehen, z.B. Arzt selbst, Servicetechniker, einige Angestellte) oder dass der Zugang zu den Räumlichkeiten durch den Leistungserbringer geeignet beschränkt wird (z.B. Patienten dürfen zwar Wartezimmer und Behandlungsräume betreten, aber nicht den Serverraum, in welchem der Konnektor aufbewahrt wird – siehe die Annahme A.phys_Schutz).

Angriffe, deren Bezeichner das Wort „remote“ enthalten (T.remote_TOE_WAN, T.remote_TOE_LAN, T.remote_VPN_Data und T.remote_admin_WAN), nehmen an, dass der Angreifer über keinen solchen Zutritt verfügt, sondern dass die Angriffe ausschließlich über das Transportnetz (z.B. Internet) erfolgen.

Angriffe, deren Bezeichner das Wort „admin“ enthalten (T.local_admin_LAN und T.remote_admin_WAN), nehmen an, dass ein Angreifer die Administrationsschnittstelle(n) des Netzkonnektors ausnutzt, um unbefugt Sicherheitseinstellungen zu verändern oder zu deaktivieren.

3.4.2.1. T.local_TOE_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.[26] 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* (siehe Abschnitt 3.1), aber auch sekundäre Werte wie Schlüssel),
- den Netzkonnektor so zu manipulieren, dass zukünftig vertrauliche *zu schützende Daten* kompromittiert werden können, oder
- den Netzkonnektor so zu manipulieren, dass zukünftig *zu schützende Daten* 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) mitbringen.

---

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

[26] 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 Primärsystem 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 Primärsystem aufbringt, beispielsweise durch Wechseldatenträger (CD, USB-Stick, etc.).

Ebenfalls betrachtet werden Angriffe, bei denen ein Angreifer den Netzkonnektor durch manipulierte Aufrufe aus dem Primärsystem-Netz in einen unsicheren Systemzustand bringt.

Application Note 39: Siehe auch Abschnitt 7.6.19.

3.4.2.2. T.remote_TOE_WAN

Ein Angreifer greift den Konnektor aus dem Transportnetz heraus an. Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer nutzt Implementierungsfehler des Netzkonnektors aus, um den Konnektor zu kompromittieren – mit allen Aspekten wie in Abschnitt 3.4.2.1 T.local_TOE_LAN beschrieben. Der Angreifer greift den Netzkonnektor unbemerkt über das Netzwerk an, um unautorisierten Zugriff auf weitere Werte zu erhalten.

3.4.2.3. T.remote_TOE_LAN

Ein Angreifer greift den Konnektor aus dem Transportnetz heraus an. Der Angreifer verfügt über hohes Angriffspotential. Ziel ist wieder eine Kompromittierung des Konnektors, mit allen Aspekten wie bereits in Abschnitt 3.4.2.1 T.local_TOE_LAN beschrieben. Im Gegensatz zur Bedrohung T.remote_TOE_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 Primärsystem zu kompromittieren und/oder im Anschluss daran den Konnektor von dessen LAN-Seite her anzugreifen. Die Kompromittierung eines Primärsystems ist gegeben, wenn ein Angreifer aus dem Transportnetz unautorisiert auf personenbezogene Daten im Primärsystem zugreifen kann oder wenn der Angreifer ein Primärsystem erfolgreich und unbemerkt manipulieren kann.

Dazu nutzt der Angreifer Implementierungsfehler 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.

Einen Spezialfall dieses Angriffs stellt das Szenario dar, dass ein Primärsystem vom Transportnetz (WAN) aus mit bösartigem Code verseucht wird und in der Folge Angriffe gegen den Konnektor an dessen LAN-seitiger Schnittstelle vornimmt. Ein Primärsystem könnte vom Transportnetz aus mit bösartigem Code verseucht werden, wenn der Netzkonnektor keine effektive Netztrennung zwischen WAN und LAN leistet.

Application Note 40: Siehe auch Abschnitt 7.6.19.

3.4.2.4. T.remote_VPN_Data

Ein Angreifer aus dem Transportnetz hört Daten ab oder manipuliert Daten unbemerkt, die zwischen dem Konnektor und der zentralen Telematikinfrastruktur (oder umgekehrt) 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 Primärsystem übertragene Daten zu erhalten.
- Ein Angreifer verändert verschlüsselte Daten während der Übertragung unbemerkt.

Für die komplementäre Bedrohung

- Ein Angreifer kann sich dem VPN-Konzentrator gegenüber als Netzkonnektor ausgeben (evtl. auch man-in-the-middle-Angriff), um unautorisierten Zugriff auf zum Primärsystem übertragene Daten zu erhalten.

gilt folgendes: Diese Bedrohung richtet sich nicht gegen den EVG (Netzkonnektor), sondern gegen den VPN-Konzentrator. Sie muss daher auch durch eine Sicherheitsfunktion des VPN-Konzentrators abgewehrt werden, und zwar durch eine vom VPN-Konzentrator erzwungene Authentisierung des EVGs gegenüber dem VPN-Konzentrator. Der EVG unterstützt dies, indem er eine solche Authentisierung durchführt – die Authentisierung im Rahmen des Aufbaus des VPN-Kanals ist gegenseitig (siehe O.VPN_Auth). Auch der Schutz vor unautorisiertem Zugriff auf zum Primärsystem übertragene Daten ist Aufgabe des VPN-Konzentrators: Er muss die Daten vor dem Versand verschlüsseln. Der Konnektor unterstützt eine solche verschlüsselte Kommunikation, indem er die Daten entschlüsselt, siehe O.VPN_Vertraul.

3.4.2.5. T.local_admin_LAN

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

Diese Bedrohung umfasst auch folgende Aspekte:

- Ein lokaler Angreifer bringt schadhafte Software auf den Netzkonnektor auf.
- Ein lokaler Angreifer greift unautorisiert auf genutzte kryptographische Schlüssel im Arbeitsspeicher des Netzkonnektors zu.
- Ein lokaler Angreifer deaktiviert die Protokollierungsfunktion des Netzkonnektors.

3.4.2.6. T.remote_admin_WAN

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

Diese Bedrohung umfasst auch folgende Aspekte:

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

3.4.2.7. T.counterfeit

Ein Angreifer bringt gefälschte Netzkonnektoren in Umlauf, ohne dass dies vom VPN-Konzentrator erkannt wird.[27] 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 erforderlich ist – oder bei der Erstauslieferung durchgeführt werden. Der Angreifer verfügt über hohes Angriffspotential. Der Angreifer verfolgt dieselben Ziele wie unter T.local_admin_LAN besprochen.

3.4.2.8. T.Zert_Prüf

Ein Angreifer manipuliert Sperrlisten, die im Rahmen der Gültigkeitsprüfung von Zertifikaten zwischen dem EVG und einem netzbasierten Dienst (siehe OE.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

[27] 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.counterfeit auf das unbemerkte Fälschen bzw. Austauschen von Netzkonnektoren.

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.

3.4.2.9. T.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 Echtzeit zu bewirken, oder gibt sich selbst als Zeitdienst aus. Der Angreifer verfügt über hohes Angriffspotential.

Application Note 41: Falls es weitere Bedrohungen gibt, die durch den Netzkonnektor abgewehrt werden, soll der ST-Autor diese explizit benennen und beschreiben.

3.5. Organisatorische Sicherheitspolitiken

Dieses Schutzprofil definiert keine organisatorischen Sicherheitspolitiken.

3.6. Annahmen

A.phys_Schutz **Physischer Schutz des Netzkonnektors („sichere Umgebung“)**
Die Umgebung schützt den EVG vor physischem Zugriff Unbefugter sowie vor Entwendung. Die Umgebung wehrt Angriffe an allen physikalischen Schnittstellen des EVGs ab.

Der Konnektor ist nicht öffentlich zugänglich. Die Umgebung stellt sicher, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass organisatorische Maßnahmen größeren Schaden abwehren können.

Die Umgebung schützt außerdem den Kommunikationskanal zwischen dem EVG und weiteren Komponenten des Konnektors.

Die Umgebung muss Schutz gegen Angreifer mit hohem Angriffspotential bieten oder ein unberechtigter Zugang muss mit hoher Sicherheit erkannt werden.

Application Note 42: Im Falle einer Mehrkomponentenlösung muss der Kommunikationskanal zwischen den Konnektor-Komponenten (z.B. Netzkonnektor und Anwendungskonnektor) organisatorisch oder technisch geschützt werden. Damit dieses Schutzprofil allgemein verwendet werden kann, wird hier nur organisatorischer Schutz (in Form der Annahme A.phys_Schutz) gefordert.

- Organisatorischer Schutz kann beispielsweise dadurch erreicht werden, dass Anwendungskonnektor und Netzkonnektor im selben zutrittsgeschützten Serverraum bzw. Rechenzentrum einer Klinik aufgestellt werden.
- Technischer Schutz kann durch kryptographische Sicherung der Kommunikation implementiert werden, beispielsweise durch einen TLS/SSL-Kanal mit vorausgehender gegenseitiger Authentisierung.

Application Note 43: **Differenzierung durch physischen Schutz:** Der ST-Autor kann die Annahme A.phys_Schutz abschwächen und weitere Sicherheitsfunktionalität vom EVG fordern. Die exakte Ausprägung von A.phys_Schutz kann ein **Differenzierungsmerkmal** zwischen verschiedenen Produkten darstellen, siehe auch Application Note 4: *Möglichkeit zur Differenzierung* und Abschnitt 7.6.7.

Vergleiche zu diesem Themenkomplex auch

- Application Note 4: Möglichkeit zur Differenzierung und
- Application Note 49: Annahmen zum physischen Schutz
- sowie die Hinweise in Abschnitt 7.6.7 und OE.phys_Schutz.

A.PF_LAN **LAN-seitiger Paketfilter**

Im Fall einer Mehrkomponentenlösung stellt die IT-Einsatzumgebung einen LAN-seitigen Paketfilter bereit, welcher den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt.

Application Note 44: Im Fall einer Einbox-Lösung soll der ST-Autor diese Annahme entfernen, siehe Abschnitt 7.6.19.

A.SM-K **Sicherheitsmodul für den Netzkonnektor (SM-K)**

Der Netzkonnektor hat Zugriff auf ein Sicherheitsmodul (SM-K), das sicher mit dem Netzkonnektor verbunden ist. Sicher bedeutet in diesem Fall, dass das SM-K nicht vom Netzkonnektor getrennt werden kann und dass die Kommunikation zwischen SM-K und Netzkonnektor weder mitgelesen noch manipuliert werden kann.
Das SM-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des Netzkonnektors repräsentiert und welches auch für O.VPN_Auth verwendet wird, und führt kryptographische Operationen mit diesem Schlüsselmaterial durch (Authentisierung), ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.
Das SM-K ist nach einem entsprechenden Schutzprofil evaluiert und zertifiziert.

Application Note 45: Siehe auch Abschnitt 7.6.13.

A.sichere_TI **Sichere Telematikinfrastruktur**

Die zentrale Telematikinfrastruktur wird als vertrauenswürdig angesehen, d.h., Angriffe aus der zentralen Telematikinfrastruktur

werden nicht betrachtet.
Die Administration der Telematikinfrastruktur sorgt 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 des VPN-Konzentrators 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.kein_DoS **Keine denial-of-service-Angriffe**
Das Transportnetz wehrt denial-of-service-Angriffe effektiv ab.

Application Note 46: Siehe auch Abschnitt 7.6.8.

A.AK **Anwendungskonnektor nutzt Netzkonnektor korrekt**
Die Primärsysteme und der Anwendungskonnektor nutzen die Sicherheitsdienste des EVG über dessen definierte Schnittstellen automatisch. Durch die Art der Aufrufe ist für den Netzkonnektor jederzeit eindeutig erkennbar, welche Informationen ausschließlich an die zentrale Telematikinfrastruktur weitergeleitet werden müssen und welche nicht.

Application Note 47: Es werden nur online-Geschäftsvorfälle überhaupt vom Anwendungskonnektor an den Netzkonnektor weitergeleitet. Aufrufe vom Anwendungskonnektor sind zur Weiterleitung in die Telematikinfrastruktur (Dienste gemäß § 291a SGB V) bestimmt. Es ist möglich, dass der Netzkonnektor über weitere VPN-Kanäle, die nicht zu Diensten gemäß § 291a SGB V führen, Mehrwertdienste bereitstellt. Der ST-Autor soll die Funktionalität des EVG einschließlich eventueller Mehrwertdienste und der dazu erforderlichen Separationsmechanismen beschreiben. – Siehe auch Abschnitte 7.6.2 und 7.6.9.

A.Betrieb_AK **Sicherer Betrieb des Anwendungskonnektors**
Der Betreiber der Primärsysteme organisiert diesen Betrieb in sicherer Art und Weise: Er setzt nur Primärsysteme und Anwendungskonnektoren ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen. Er administriert die Primärsysteme und Anwendungskonnektoren in sicherer Art und Weise. Er trägt die Verantwortung dafür, dass der Anwendungskonnektor den Netzkonnektor in der spezifizierten Art und Weise nutzt, also insbesondere die spezifizierten Schnittstellen korrekt nutzt. 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) keine Schadsoftware auf die Primärsysteme aufgebracht wird. Er ist verantwortlich dafür,

dass eine Anbindung der Primärsysteme an potentiell unsichere Netze (z.B. Internet) unterbunden wird oder 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 Netzkonnektor keine weiteren ungeschützten oder schlechter geschützten Zugänge zum Transportnetz gibt.

Die Verantwortung für die Primärsysteme liegt sowohl beim Leistungserbringer (der z.B. lokal potentiell bösartige Software oder auch potentiell fehlerhafte Updates der Primärsystem-Software einspielen könnte) als auch beim Primärsystem-Hersteller (der z.B. den korrekten Aufruf der Konnektor-Schnittstellen sicherstellen muss) – aber in jedem Fall außerhalb des Konnektors.

A.Admin_EVG **Sichere Administration des EVG**
Der Betreiber des EVG sorgt dafür, dass administrative Tätigkeiten (dies umfasst sowohl die lokale als auch die optionale zentrale Administration) in Übereinstimmung mit der Administrator-Dokumentation des EVG durchgeführt werden. Insbesondere ist für diese Tätigkeiten vertrauenswürdiges 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.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.

4. Sicherheitsziele

4.1. Sicherheitsziele für den TOE (EVG)

Der EVG muss – wie im Folgenden detaillierter dargestellt – die Nutzdaten (*zu schützende Daten*, siehe Abschnitt 3.1), die Primärsysteme und sich selbst schützen.

4.1.1. Allgemeine Ziele: Schutz und Administration

O.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 EVG erfolgen (aber: siehe OE.phys_Schutz).
Der EVG führt beim Start-up und bei Bedarf Selbsttests durch.
Der EVG schützt die von ihm in einem sicheren Schlüsselspeicher gespeicherten Geheimnisse gegen Auslesen und jegliche andere unbefugte Kenntnisnahme.
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.

Application Note 48: Der EVG nutzt den sicheren Schlüsselspeicher zur Speicherung eigener Geheimnisse; siehe auch die Ausführungen zum sicheren Schlüsselspeicher unten in Abschnitt 5.1.1.5 unter der Zwischenüberschrift Sicherer Schlüsselspeicher.

Application Note 49: **Annahmen zum physischen Schutz:** In diesem Schutzprofil wird Schutz vor physischen Angriffen durch die Einsatzumgebung angenommen (siehe A.phys_Schutz). Falls der EVG aus Hardware und Software besteht, kann der ST-Autor optional fordern, dass der EVG physische Angriffe abwehrt oder diese erkennbar macht. In diesem Fall kann die Annahme A.phys_Schutz abgeschwächt werden oder entfallen. Falls der EVG auch Schutz vor physischen Angriffen bieten soll (d.h.: falls der EVG ein sicheres Gehäuse postuliert), umfassen die sicherheitstechnischen Veränderungen in O.Schutz auch physische Manipulationen. Der ST-Autor soll in einem solchen Fall das Ziel O.Schutz im Security Target geeignet erweitern.

Vergleiche zu diesem Themenkomplex auch

- Application Note 4: Möglichkeit zur Differenzierung und
- Application Note 43: Differenzierung durch physischen Schutz sowie
- Abschnitt 7.6.7.

O.TOE_Authenticity Authentizität des Netzkonnektors

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

Application Note 50: Siehe auch Abschnitt 7.6.11.

O.Admin_EVG Administration nur nach I&A und über sicheren Kanal

Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen. Dazu ermöglicht der EVG die sichere Identifikation und Authentisierung eines Administrators, welcher die lokale und/oder (optional) entfernte Administration des EVG durchführen kann. Die Administration erfolgt rollenbasiert. Für den Fall, dass die Administration nicht über einen dedizierten lokalen Anschluss (PS3), sondern über Netzverbindungen (lokal über PS1 oder zentral über PS2) 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).

Zu den administrativen Funktionen gehört unter anderem das Aktivieren und Deaktivieren der Protokollierungsfunktion (siehe O.Protokoll).

Application Note 51: Der EVG muss mindestens die Rolle Administrator unterstützen, bei Bedarf ist auch ein abgestuftes rollenbasiertes Administrationskonzept umzusetzen (getrennte Zugangskennungen, unterschiedliche Administrationsrechte).

O.Protokoll Protokollierung mit Zeitstempel

Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit. Der für das Protokoll erforderliche Zeitstempel wird dabei durch O.Zeit bereitgestellt.

Application Note 52: Eine Protokollierung von Zugriffen auf medizinische Daten nach § 291 a (6) Satz 2 SGB V erfolgt durch den Anwendungskonnektor (auf der eGK oder in der zentralen Telematikinfrastruktur). Diese Art der Protokollierung ist hier nicht gemeint; der Netzkonnektor ist in die Protokollierung von Zugriffen nicht involviert.

O.Update Sichere Update-Funktionalität

Der EVG bietet die Möglichkeit, Aktualisierungen (Updates) auf sicherem Wege entgegen zu nehmen. Updates werden erst aktiviert, wenn die Datenintegrität und die Authentizität des Absenders

erfolgreich verifiziert werden konnten (Signaturprüfung). Beim Scheitern eines Updates bleibt die alte Version der Software aktiv und intakt. Siehe auch OE.Update. Updates müssen offline eingespielt werden können, d.h., unter Kontrolle des lokalen Administrators.

Application Note 53: Abhängig von der Sicherheitspolitik kann es erforderlich sein, auch die Vertraulichkeit der Updates durch eine Verschlüsselung zu schützen. Falls dies gewünscht wird, soll der ST-Autor die Ziele O.Update und OE.Update entsprechend ergänzen und die erforderlichen funktionalen Anforderungen in das ST aufnehmen (z.B. Aufnahme einer weiteren Anforderung FCS_COP.1/... oder Modifikation der vorhandenen Anforderung FCS_COP.1/Encrypt).

O.Zeit **Sichere Systemzeit**
Der Konnektor verfügt über eine verlässliche Systemzeit, die in regelmäßigen Abständen über einen sicheren Kanal mit einem vertrauenswürdigen Zeitserver synchronisiert wird (siehe OE.Zeitsynchro).

Die sichere Systemzeit wird unter anderem dazu verwendet, die Gültigkeit von Zertifikaten (in diesem Fall: Zertifikate für VPN-Schlüssel sowie evtl. für Schlüssel anderer sicherer Kanäle) zu überprüfen. Da der Zeitserver innerhalb der zentralen Telematikinfrastruktur bereitgestellt wird, dient bereits der VPN-Tunnel zu den VPN-Konzentratoren für Dienste gemäß § 291 a SGB V als sicherer Kanal.

4.1.2. Ziele für die VPN-Funktionalität

O.VPN_Auth **Authentisierung der Kommunikationspartner des VPN-Tunnels**
Der EVG erzwingt eine gegenseitige Authentisierung der Kommunikationspartner des VPN-Tunnels (Netzkonnektor und VPN-Konzentrator in der zentralen Telematikinfrastruktur). Der Netzkonnektor prüft die Authentizität des VPN-Konzentrators; das dazu erforderliche Schlüsselmaterial bezieht der Netzkonnektor vom SM-K. Der Netzkonnektor authentisiert sich gegenüber dem VPN-Konzentrator; das dazu erforderliche Schlüsselmaterial bezieht der Netzkonnektor ebenfalls vom SM-K.

Application Note 54: Bei dem erforderlichen Schlüsselmaterial kann es sich z.B. um folgende Schlüssel handeln:

- Authentisierung des Netzkonnektors: ein privater Authentisierungsschlüssel mit passendem Zertifikat in der Geräte-PKI,
- Prüfung der Authentizität des VPN-Konzentrators: ein öffentlicher Schlüssel oder ein Zertifikat der Wurzel (Root) der Geräte-PKI.

Beide Schlüssel sollten sinnvollerweise auf dem SM-K gespeichert sein: Zugelassene VPN-Konzentrator werden nach Konnektor-Spezifikation [20] in sogenannten Trusted Server Lists (TSLs) gespeichert werden. Der Vertrauensanker für die TSLs (Gematik Root-CA) sollte im SM-K gespeichert sein. Für die TSLs selber ist dies nicht erforderlich, sofern der Konnektor deren Integrität zu gegebener Zeit mittels des Vertrauensankers überprüft.

O.Zert_Prüf **Gültigkeitsprüfung für VPN-Zertifikate**
Der EVG ermöglicht eine Gültigkeitsprüfung für die Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden. Die Zertifikate müssen mathematisch geprüft und mit Sperrlisten (Certificate Revocation Lists, CRLs) abgeglichen werden.

O.VPN_Vertraul **Schutz der Vertraulichkeit von Daten im VPN-Tunnel**
Der EVG schützt die Vertraulichkeit der Nutzdaten[28] bei der Übertragung von und zu den VPN-Konzentratoren.
Bei der Übertragung der Nutzdaten zwischen Netzkonnektor und entfernten VPN-Konzentratoren soll der Konnektor die Nutzdaten verschlüsseln (vor dem Versand) bzw. entschlüsseln (nach dem Empfang); dies soll durch die Verwendung des IPsec-Protokolls erreicht werden.
Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.
Der EVG verfügt über eine für den Benutzer leicht zugängliche Anzeige, die ihm die Betriebsbereitschaft sowie das Bestehen oder Nichtbestehen einer sicheren VPN-Verbindung zur zentralen Telematikinfrastruktur signalisiert.[29]

O.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 Netzkonnektor und entfernten VPN-Konzentratoren soll der Konnektor die Integrität der Nutzdaten sichern (vor dem Versand) bzw. prüfen (nach dem

[28] Der Begriff „Nutzdaten“ schließt in diesem PP grundsätzlich auch die Verkehrsdaten mit ein, also Daten über Kommunikationsbeziehungen bzw. Daten darüber, welcher Versicherte zu welchem Zeitpunkt bei welchem Leistungserbringer Leistungen in Anspruch genommen hat.

[29] Der Anwender des Netzkonnektors (EVGs) soll bei der Inbetriebnahme und Einrichtung des Netzkonnektors leicht (z.B. durch Blick auf eine LED) prüfen können, ob der Verbindungsaufbau zur Telematikinfrastruktur erfolgreich und sicher (d.h. authentisch, verschlüsselt und integritätsgeschützt) erfolgt. Wenn der EVG derart betriebsbereit eingerichtet worden ist, dass er bei Bedarf stets selbständig sichere Verbindungen aufbaut, muss der Anwender diese Anzeige fortan nicht mehr kontinuierlich überprüfen, so dass der EVG auch an einem sicheren Ort aufbewahrt werden kann, der den leichten Zugang zur Anzeige erschwert.

Empfang); dies soll durch die Verwendung des IPsec-Protokolls erreicht werden.
Der EVG verfügt über eine für den Benutzer leicht zugängliche Anzeige, die ihm die Betriebsbereitschaft sowie das Bestehen oder Nichtbestehen einer sicheren VPN-Verbindung zur zentralen Telematikinfrastruktur signalisiert.

4.1.3. Ziele für die Paketfilter-Funktionalität

O.PF_WAN **Dynamischer Paketfilter zum WAN**
Der EVG schützt sich selbst, andere Konnektorteile und die Primärsysteme vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN). Es werden Angreifer mit hohem Angriffspotential betrachtet.

O.PF_LAN **Dynamischer Paketfilter zum LAN**
Der EVG schützt sich selbst 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* erzwingt der EVG die Nutzung des VPN-Tunnels. Ungeschützter Zugriff auf das Transportnetz wird durch den EVG unterbunden.

Application Note 55: Der EVG muss in der Lage sein, *zu schützende Daten* zu erkennen; siehe dazu OE.AK. Zugriff auf durch das Transportnetz angebotene Mehrwertdienste darf nur unter der Vermittlung durch geeignete Dienste (z.B. Proxies) der zentralen Telematikinfrastruktur ermöglicht werden.

Siehe auch Abschnitt 7.6.8 (denial-of-service) und 7.6.16 (sichere Kanäle).

Application Note 56: Im Fall einer Einbox-Lösung ist dieses Ziel so zu erweitern, dass der LAN-seitige Paketfilter des Netzkonnektors nicht nur den Netzkonnektor selbst, sondern auch den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt; siehe dazu auch Abschnitt 7.6.19.

O.Stateful **Stateful Packet Inspection (zustandsgesteuerte Filterung)**
Der EVG bietet grundlegende Intrusion Prevention-Funktionalität. Er implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter. Der Netzkonnektor schreibt Audit-Daten zur zeitnahen Auswertung mit dem Ziel grundlegender Intrusion Prevention (stateful packet inspection, siehe Application Note 23:).

Application Note 57: Eine solche Auswertung mit dem Ziel Intrusion Prevention kann prinzipiell sowohl für den WAN-seitigen Paketfilter (O.PF_WAN) als auch für den LAN-seitigen Paketfilter (O.PF_LAN) durchgeführt werden.

Gefordert wird an dieser Stelle nur die zustandsgesteuerte Filterung; nachdem eine Verbindung beendet wurde, können sämtliche Protokolldaten über ihren Zustand gelöscht werden. Eine weitergehende (spätere) Auswertung des Protokolls (über die grundlegende Intrusion Prevention hinaus) kann optional durch die IT-Umgebung erfolgen (siehe Application Note 128:).

Eine Protokollierung von Zugriffen auf medizinische Daten nach § 291 a (6) Satz 2 SGB V erfolgt durch den Anwendungskonnektor. Diese Art der Protokollierung ist hier nicht gemeint. Auch die Protokollierung sicherheitsrelevanter Ereignisse im Security Log (siehe O.Protokoll) ist an dieser Stelle nicht gemeint.

4.2. Sicherheitsziele für die Umgebung

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

OE.RNG **Externer Zufallszahlengenerator**
Die Umgebung stellt dem Netzkonnektor einen externen Zufallszahlengenerator bereit, der Zufallszahlen geprüfter Güte und Qualität liefert.

Application Note 58: Siehe auch Abschnitt 7.6.10.

OE.Zeitsynchro **Zeitsynchronisation**
Die IT-Umgebung muss Dienste bereitstellen, mit deren Hilfe der Netzkonnektor seine Systemzeit synchronisieren kann. Der Dienst muss über eine verlässliche Systemzeit verfügen.

OE.PF_LAN **LAN-seitiger Paketfilter**
Im Fall einer Mehrkomponentenlösung stellt die IT-Einsatzumgebung einen LAN-seitigen Paketfilter bereit, welcher den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt.

Application Note 59: Im Fall einer Einbox-Lösung soll der ST-Autor dieses Umgebungsziel entfernen, siehe Abschnitt 7.6.19.

OE.SM-K **Sicherheitsmodul SM-K stellt kryptographische Identität bereit**
Der Netzkonnektor hat Zugriff auf ein Sicherheitsmodul (SM-K), das sicher mit dem Netzkonnektor verbunden ist. Sicher bedeutet in diesem Fall, dass das SM-K nicht vom Netzkonnektor getrennt werden kann

und dass die Kommunikation zwischen SM-K und Netzkonnektor weder mitgelesen noch manipuliert werden kann.
Das SM-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des Netzkonnektors repräsentiert und welches auch für O.VPN_Auth verwendet wird, und führt kryptographische Operationen mit diesem Schlüsselmaterial durch (Authentisierung), ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.
Das SM-K ist nach einem entsprechenden Schutzprofil evaluiert und zertifiziert. Der Hersteller des Netzkonnektors darf nur nach diesem Schutzprofil evaluierte und zertifizierte Sicherheitsmodule SM-K in sein Produkt integrieren.

Application Note 60: Siehe auch Abschnitt 7.6.13.

OE.AK **Datenkennzeichnung durch Anwendungskonnektor**
Die Hersteller von Anwendungskonnektoren müssen ihre Produkte so gestalten, dass der Anwendungskonnektor *zu schützende Daten*, die durch Dienste gemäß § 291 a SGB V verarbeitet werden sollen, als solche für den Netzkonnektor erkennbar macht, so dass der Netzkonnektor *zu schützende Daten* in korrekter Weise über den entsprechenden VPN-Tunnel für Dienste gemäß § 291a SGB V (zu den *VPN-Konzentratoren für Dienste gemäß § 291 a SGB V*, siehe Abschnitt 7.6.15 Arten von VPN-Konzentratoren) versendet. Sie müssen die spezifizierten Netzkonnektor-Schnittstellen verwenden und die entsprechenden Datenformate einhalten.
Dazu müssen die Entwickler von Anwendungskonnektoren die entsprechenden Vorschriften beachten und die vom Netzkonnektor bereitgestellten Schnittstellen geeignet verwenden, so dass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

Application Note 61: Siehe auch Abschnitt 7.6.14.

OE.Admin_EVG **Sichere Administration des EVG**
Der Betreiber des EVG muss dafür sorgen, dass administrative Tätigkeiten der lokalen und zentralen Administration in Übereinstimmung mit der Administrator-Dokumentation des EVGs durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges und ausgebildetes Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen und –token (z.B. PIN bzw. Passwort oder Schlüssel-Token) geheimhalten bzw. dürfen diese nicht weitergeben.

OE.PKI **Betrieb einer Public-Key-Infrastruktur und Sperrlisten-Verteilung**
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. Dies kann sowohl durch Bereitstellung von Online-Abfragemöglichkeiten (z.B. OCSP) erreicht werden als auch durch die zeitnahe Verteilung von Sperrlisten (Certificate Revocation Lists, CRLs). Die Auskünfte der Public-Key-Infrastruktur werden von der Infrastruktur signiert. Dieses Umgebungsziel unterstützt O.Zert_Prüf. Die Infrastruktur soll hinreichend hoch verfügbar sein.

Application Note 62: Der EVG unterstützt gemäß der zum Zeitpunkt der Erstellung dieses Schutzprofils gültigen Konnektor-Spezifikation [20] nur die Prüfung mit Hilfe von Sperrlisten; OCSP-Abfragen werden vom EVG nicht gefordert.

OE.phys_Schutz **Physischer Schutz des Netzkonnektors**
Die Umgebung muss den Konnektor vor physischem Zugriff Unbefugter sowie vor Entwendung schützen. Die Umgebung muss Angriffe an allen physikalischen Schnittstellen des EVGs abwehren.

Der Konnektor darf nicht öffentlich zugänglich sein (z.B. Aufbewahrung in einem nicht öffentlich zugänglichen Raum). Die Umgebung muss sicherstellen, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass organisatorische Maßnahmen größeren Schaden abwehren können.

Die Umgebung muss außerdem den Kommunikationskanal zwischen dem EVG und weiteren Komponenten des Konnektors schützen.

Die Umgebung muss Schutz gegen Angreifer mit hohem Angriffspotential bieten oder ein unberechtigter Zugang muss mit hoher Sicherheit erkannt werden.

Application Note 63: Siehe auch Abschnitt 7.6.7 und A.phys_Schutz.

OE.sichere_TI **Sichere Telematikinfrastruktur**
Der Betreiber der zentralen Telematikinfrastruktur muss sicherstellen, dass aus dem VPN-Netz heraus keine Angriffe gegen den Konnektor durchgeführt werden. Die Administration der Telematikinfrastruktur muss 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.kein_DoS **Keine denial-of-service-Angriffe**
Die Betreiber der zentralen Telematikinfrastruktur müssen geeignete Gegenmaßnahmen treffen, um denial-of-service-Angriffe aus dem Transportnetz gegen die zentrale Telematikinfrastruktur abzuwehren.

Application Note 64: Durch die explizite Erwähnung dieses Umgebungsziels wird deutlich abgegrenzt, welche Leistungen der EVG nicht erbringen kann bzw. wo er nur unterstützend tätig werden kann. Siehe auch Abschnitt 7.6.8.

OE.Betrieb_AK **Sicherer Betrieb des Anwendungskonnektors**
Der Betreiber des Anwendungskonnektors und der Primärsysteme muss diesen Betrieb in sicherer Art und Weise organisieren: Er setzt nur Anwendungskonnektoren und Primärsysteme ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen. Er administriert die Anwendungskonnektoren und Primärsysteme in sicherer Art und Weise. Er trägt die Verantwortung dafür, dass die Anwendungskonnektoren und Primärsysteme den Netzkonnektor 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 Primärsysteme aufgebracht wird. Er ist verantwortlich dafür, dass die Primärsysteme in sicherer Weise an potentiell unsichere Netze (z.B. Internet) angebunden sind.

Application Note 65: **Schutz des Anwendungskonnektors vor LAN-seitigen Angriffen:** Falls der Konnektor als Mehrkomponentenlösung ausgestaltet wird, kann der Netzkonnektor nicht in jedem Fall sicherstellen, dass er den Anwendungskonnektor vor Angriffen aus dem LAN schützt. Falls (z.B. aufgrund der Netztopologie des konkreten Produkts) der Schutz des Anwendungskonnektors nicht durch den Netzkonnektor gewährleistet werden kann, muss der Betreiber des Anwendungskonnektor diesen durch eine gesonderte Komponente (Paketfilter) sichern. Diese Komponente muss eine vergleichbar hohe Sicherheit bieten wie der Netzkonnektor. Der ST-Autor muss das ST geeignet anpassen.

OE.Update **Prozesse für sicheres Software-Update**
Es müssen Prozesse etabliert werden, die dafür sorgen, dass Software-Updates nur dann signiert und ausgeliefert werden, wenn der Code von einer dazu autorisierten Stelle inspiziert wurde (Code Review). Der EVG (Netzkonnektor) muss bereits vor seiner Auslieferung (d.h. üblicherweise während der Produktion) mit einem Prüfschlüssel versehen werden, so dass er später im Feld die Integrität und Authentizität signierter Updates prüfen kann. Das Schlüsselpaar muss von geeigneter kryptographischer Qualität sein.

Application Note 66: Siehe auch O.Update und Application Note 53: (optional: verschlüsselte Updates).

OE.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.

5. Sicherheitsanforderungen

5.1. EVG-Sicherheitsanforderungen

5.1.1. Funktionale EVG-Sicherheitsanforderungen

Die funktionalen Sicherheitsanforderungen werden im Folgenden nicht wie sonst häufig in alphabetischer Reihenfolge aufgezählt, sondern nach funktionalen Gruppen gegliedert. Dadurch soll ein besseres Verständnis der Anforderungen und ihrer Abhängigkeiten untereinander erreicht werden. Die funktionalen Gruppen orientieren sich an den in Abschnitt 2.4 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

- VPN-Client: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);
- dynamischer Paketfilter: sowohl für WAN als auch für LAN, Separation von Mehrwertdiensten, grundlegende Intrusion Prevention;
- Netzdienste: Echtzeituhr, Zeitsynchronisation über sicheren Kanal, Zertifikatsprüfung mittels Sperrlisten;
- Stateful Packet Inspection: Generierung von Audit-Daten für spätere Intrusion Prevention;
- Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, Ereignisprotokollierung (Sicherheits-Log, Security Log);
- Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, sicheres Software-Update.

Eine tabellarische Abbildung der Sicherheitsdienste aus Abschnitt 2.4 auf die EVG-Sicherheitsziele aus Abschnitt 4.1 und von dort auf die im Folgenden detailliert beschriebenen funktionalen Sicherheitsanforderungen findet sich in Abschnitt 6.2.1, Tabelle 6: Abbildung der Sicherheitsdienste auf Ziele und Anforderungen.

Um die Semantik von Sicherheitsanforderungen leichter erkennen zu können, wurden den Anforderungen teilweise **Suffixe** angehängt, z.B. „/VPN“ für den Trusted Channel, der den VPN-Kanal fordert (siehe FTP_ITC.1/VPN). Diese Vorgehensweise erleichtert es auch, zusammenhängende Anforderungen zu gruppieren (z.B. FDP_IFC.1/PF, FDP_IFF.1/PF und FMT_MSA.3/PF sowie FDP_ACC.1/KeySt, FDP_ACF.1/KeySt, FMT_MSA.3/KeySt und FMT_MSA.1/KeySt) und iterierte Komponenten zu unterscheiden (z.B. FPT_TDC.1/Time und FPT_TDC.1/Zert sowie FAU_GEN.1/Audit und FAU_GEN.1/Stateful). Durch die Verwendung der Suffixe wird außerdem eine leichte Unterscheidbarkeit von Anforderungen, die sowohl an den EVG (TOE) als auch an die IT-Umgebung (IT Environment) gerichtet werden (z.B. FPT_STM.1/TOE und FPT_STM.1/Env), möglich.

5.1.1.1. VPN-Client

VPN

Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Um die Sicherheitsanforderungen, die wesentlich durch den VPN-Client bedingt werden, leicht erkennen zu können, wurden diese Sicherheitsanforderungen durch das Suffix „/VPN“ gekennzeichnet.

FTP_ITC.1/VPN	**Inter-TSF trusted channel**
Dependencies:	No dependencies.
FTP_ITC.1.1/VPN	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification *and*[30] disclosure.
FTP_ITC.1.2/VPN	The TSF shall permit *the TSF and the remote trusted IT product*[31] to initiate communication via the trusted channel.
FTP_ITC.1.3/VPN	The TSF shall initiate communication via the trusted channel for *VSDD and VODD, [*assignment*: list of functions for which a trusted channel is required (may be empty)*]*[32].
Refinement:	Die Anforderung „protection of the channel data from modification and disclosure“ in FTP_ITC.1.1/VPN ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Der Trusted Channel muss auf Basis des **IPsec**-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [20]). Zusätzlich soll **NAT-Traversal** unterstützt werden. Die bereits teilweise vorgenommene Zuweisung (assignment) „*VSDD and VODD*“ bezeichnet die Dienste Versichertenstammdatendienst und Verordnungsdatendienst (siehe dazu das Glossar [31]).
Application Note 67:	Der Netzkonnektor **muss RFC 2409 (IKE v1)** [37] **und soll RFC 4306 (IKEv2)** [38] unterstützen, siehe Konnektor-Spezifikation [20], Version 2.0.0, Abschnitt 4.1, Anforderungen AF_KON_026 (NAT-Traversal), AF_KON_027 (IPSec/IKEv1), AF_KON_028 (IKEv2, IPv6 sowie IPv6-Tunneling) und AF_KON_040 (Konformität von IPSec-Subsystem zu RFCs) sowie Abschnitte 4.1.6.3 (Netzdienste / Anbindung des Konnektors an die Telematikinfrastruktur) und 4.1.6.9 (Netzdienste / Netzwerkfunktionalität des Konnektors). Man beachte, dass **RFC 4306 (IKEv2)** [38] noch den Status „proposed“ besitzt. Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit der jeweils gültigen Konnektor-Spezifikation [20] vornehmen.

[30] refinement (or → and)

[31] selection: *the TSF, the remote trusted IT product*

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

Application Note 68: Eine theoretisch mögliche Kommunikation von Netzkonnektoren untereinander wird in diesem Schutzprofil nicht behandelt. Falls ein Produkt eine solche Funktionalität bietet, darf sie die Sicherheit der Anwendungen gemäß § 291 a SGB V nicht beeinträchtigen.

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

Der von O.VPN_Vertraul und O.VPN_Integrität geforderte Schutz der Vertraulichkeit und Datenintegrität der Nutzdaten wird ebenfalls durch FTP_ITC.1.1/VPN 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.

Der EVG muss über eine für den Benutzer leicht zugängliche Anzeige verfügen, die ihm die Betriebsbereitschaft sowie das Bestehen oder Nichtbestehen einer sicheren VPN-Verbindung zur zentralen Telematikinfrastruktur signalisiert (siehe Anforderung aus Abschnitt 2.3).

FMT_MOF.1 **Management of security functions behaviour**

Betriebsbereitschaftsanzeige, Anzeige und Management des VPN-Verbindungsstatus'

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to *perform the operations listed in the table below (in column "Operation") on*[33] the functions *listed in the table below (in column "Funktion")*[34] to *the roles identified in the table below (in column "zulässig für Rolle...")*[35].

Funktion	Operation	zulässig für Rolle...
Betriebs-bereitschaft	Feststellen der Betriebsbereitschaft (*determine the behaviour of*)	alle lokalen Benutzer mit physischem Zugang zum Gerät, [assignment: *other authorised identified roles (list may be empty)*]

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

[34] assignment: *list of functions*

[35] assignment: *the authorised identified roles*

Funktion	Operation	zulässig für Rolle...
VPN-Verbindung	Anzeige des VPN-Verbindungsstatus (Feststellen, ob eine Verbindung besteht, *determine the behaviour of*)	alle lokalen Benutzer mit physischem Zugang zum Gerät, [assignment: *other authorised identified roles (list may be empty)*]
	Anzeige des Betriebsmodus (offline oder online , *determine the behaviour of*)	alle lokalen Benutzer mit physischem Zugang zum Gerät, [assignment: *other authorised identified roles (list may be empty)*]
	aufbauen (*enable VPN connection*)	[assignment: *the authorised identified roles*]
	trennen (*disable VPN connection*)	[assignment: *the authorised identified roles*]
Ereignis-protokoll (Security Log)	abschalten, verändern (*disable, modify*),	no role

Application Note 69: Ein Ziel dieser Anforderung ist es, die Anzeige von Betriebsbereitschaft, VPN-Verbindungsstatus und Betriebsmodus (offline oder online) als funktionale Anforderung zu formulieren. Der Betriebsmodus online umfasst das Bestehen der VPN-Verbindung und die gleichzeitige Verfügbarkeit der Dienste in der zentralen Telematikinfrastruktur.

Das Ereignisprotokoll (Security Log) bezieht sich auf die Anforderung FAU_GEN.1/Audit. Die Protokollierung darf auch durch den Administrator nicht abschaltbar sein und die Protokolldaten dürfen vom Administrator nicht verändert werden können.

Der EVG kann optional auch ein komplexeres Rollenmodell unterstützen, etwa mit einer gesonderten Auditor-Rolle.

Informationsflusskontrolle

Regelbasiert müssen alle schützenswerten Informationsflüsse den etablierten VPN-Tunnel nutzen. Der ungeschützte Zugriff auf das Transportnetz wird verboten. Nur Informationsflüsse, die vom Anwendungskonnektor initiiert wurden, dürfen den VPN-Tunnel benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale Telematikinfrastruktur.

Dieser Aspekt ergibt sich zwar aus der Betrachtung des VPN-Kanals (aufgrund der Frage: Wie wird der Eingang in den VPN-Tunnel geschützt?), er wird aber im Hinblick auf seine

Realisierung der Anforderung nach Informationsflusskontrolle mittels einem dynamischen Paketfilter (FDP_IFC.1/PF, FDP_IFF.1/PF, siehe unten in Abschnitt 5.1.1.2) zugeordnet; das „PF“ steht dabei für Paketfilter. Daher finden sich die Anforderungen (TSFR) zu diesem Aspekt im nächsten Abschnitt 5.1.1.2.

Erläuterung: Die von O.PF_WAN und O.PF_LAN erzwungene VPN-Nutzung für *zu schützende Daten* (im Sinne des Abschnitts 3.1) wird durch FDP_IFF.1.2/PF umgesetzt, sofern die Paketfilter-Regeln geeignet gesetzt sind, was wiederum durch die Administratordokumentation (siehe das Refinement zu AGD_ADM.1 in Abschnitt 5.1.2) sichergestellt wird.

5.1.1.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung und grundlegender Intrusion Prevention-Funktionalität

Dynamischer Paketfilter

Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird hier als Informationsflusskontrolle modelliert (siehe FDP_IFC.1/PF und die sich daraus ergebenden Abhängigkeiten). Alle funktionalen Anforderungen, die mit dem Paketfilter in direktem Zusammenhang stehen, wurden mit dem Suffix „/PF“ (wie Paketfilter) versehen. Die zustandsgesteuerte Filterung wird in Abschnitt 5.1.1.4 Stateful Packet Inspection detailliert beschrieben.

FDP_IFC.1/PF	**Subset information flow control**
Dependencies:	FDP_IFF.1 Simple security attributes hier erfüllt durch: FDP_IFF.1/PF
FDP_IFC.1.1/PF	The TSF shall enforce the *packet filtering SFP (PF SFP)*[36] on *the subjects VPN concentrator and attacker communicating with the TOE from its WAN interface (PS2) and the subjects application connector and workstation communicating with the TOE from its LAN interface (PS1) and all incoming and outgoing information flows (inbound and outbound IP[37] traffic) between (i) the LAN and the TOE, (ii) the LAN and the WAN, (iii) the WAN and the TOE, and (iv) the WAN and the LAN*[38].

[36] assignment: *information flow control SFP*

[37] IP = Internet Protocol

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

Application Note 70: Die dynamischen Paketfilter (LAN-seitig und WAN-seitig) sollen sowohl den EVG vor Angriffen bzw. vor unerlaubten Informationsflüssen (i) aus dem LAN und (iii) aus dem WAN schützen als auch die Informationsflüsse zwischen (ii) LAN und WAN bzw. (iv) zwischen WAN und LAN kontrollieren.

Im Fall einer Einbox-Lösung muss der Netzkonnektor den Anwendungskonnektor durch einen dynamischen Paketfilter vor Angriffen aus dem LAN schützen. Im Fall einer Mehrkomponentenlösung kann dieser Schutz auch durch eine externe Komponente erbracht werden. Der ST-Autor muss das Security Target entsprechend anpassen, vgl. auch Abschnitt 7.6.19.

Application Note 71: Systembedingt bietet IPv4 (Internet Protocol, Version 4) nur eine Identifikation der Informationsflüsse, aber keine Authentisierung. Aus Mangel an besseren Mechanismen müssen dennoch auf dieser Basis die Entscheidungen über die Zulässigkeit von Informationsflüssen getroffen werden.

FDP_IFF.1/PF	**Simple security attributes**
Dependencies:	FDP_IFC.1 Subset information flow control hier erfüllt durch: FDP_IFC.1/PF FMT_MSA.3 Static attribute initialisation hier erfüllt durch: FMT_MSA.3/PF (Verwaltung der Filterregeln)
FDP_IFF.1.1/PF	The TSF shall enforce the *PF SFP*[39] based on the following types of subject and information security attributes: *For all subjects and information as specified in* FDP_IFC.1/PF*, the decision shall be based on the following security attributes: IP address, port number, and protocol type.*[40].
FDP_IFF.1.2/PF	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *For every operation (inbound or outbound, i.e. receiving or outgoing) 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.*[41]

Application Note 72: Bei Wahl eines geeigneten Satzes von Paketfilter-Regeln (siehe das Refinement zu AGD_ADM.1 in Abschnitt 5.1.2) erzwingt FDP_IFF.1.2/PF die VPN-Nutzung für *zu schützende Daten* (im Sinne des Abschnitts 3.1).

---

[39] assignment: *information flow control SFP*

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

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

FDP_IFF.1.3/PF The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4/PF The TSF shall provide the following *additional SFP capabilities: Stateful Packet Inspection,* [assignment: *list of additional SFP capabilities*][42].

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

Application Note 73: Dazu muss der EVG Informationen über eine (kurze) Historie der Verbindung verwalten. Beispielsweise werden eingehende Verbindungen üblicherweise nur als Antworten auf zuvor ausgegangene Anfragen zugelassen, so dass ein ungefragter Verbindungsaufbau aus dem WAN wirkungsvoll verhindert wird.

FDP_IFF.1.5/PF The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.6/PF The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

Application Note 74: Die dynamische Paketfilterung soll die Menge der **zulässigen Protokolle** geeignet beschränken. Der ST-Autor muss die zulässigen Protokolle in Anlehnung an die Spezifikation Netzwerksicherheit [gemNetSich] [24] benennen (vgl. dort insbesondere die Tabelle „Regelsätze/Rulesets für den Konnektor“). Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Primärsysteme.

Der ST-Autor kann mittels FDP_IFF.1.3/PF bis FDP_IFF.1.6/PF weitere Regeln ergänzen, die der EVG umsetzt. Mindestens sollen die Anforderungen an die in O.PF_LAN beschriebene **Informationsflusskontrolle** an dieser Stelle formuliert werden (EVG erzwingt, dass *zu schützende Daten* über das VPN versendet werden, EVG verhindert ungeschützten Zugriff auf das Transportnetz; siehe auch Application Note 55:). Darüber hinaus können weitere Regeln ergänzt werden, etwa weitere Plausibilitätskontrollen; dies ist aber nicht zwingend erforderlich: Bei einem assignment ist auch die Auswahl von *none* zulässig.

Erläuterung: Der von O.PF_WAN und O.PF_LAN geforderte dynamische Paketfilter wird durch FDP_IFC.1/PF und FDP_IFF.1/PF gefordert. Der Schutz vor Angriffen aus dem WAN findet sich in den Punkten (iii) und (iv) von FDP_IFC.1.1/PF, der Schutz vor Angriffen aus dem LAN in den Punkten (i) und (ii) desselben Elements. Die geforderte Eigenschaft der zustandsgesteuerten Filterung (stateful packet inspection) wird durch FDP_IFF.1.4/PF und das zugehörige Refinement gefordert.

[42] [assignment: *list of additional SFP capabilities*]

Die von FDP_IFF.1.2/PF geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (FMT_MSA.3/PF) und können vom Administrator verwaltet werden (FMT_MSA.1/PF, siehe Abschnitt 5.1.1.6 Administration).

Application Note 75: Zu den Filterregeln siehe auch *Netzwerkspezifikation [gemNet]* [23] und *Spezifikation Netzwerksicherheit [gemNetSich]* [24].

FMT_MSA.3/PF	**Static attribute initialisation**
Dependencies:	FMT_MSA.1 Management of security attributes hier erfüllt durch: FMT_MSA.1/PF FMT_SMR.1 Security roles hier erfüllt durch: FMT_SMR.1
FMT_MSA.3.1/PF	The TSF shall enforce the *PF SFP*[43] to provide *restrictive*[44] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/PF	The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Refinement:	Bei den Sicherheitsattributen handelt es sich um die Filterregeln für den dynamischen Paketfilter (FDP_IFF.1.2/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.

Application Note 76: In FMT_MSA.3.2/PF soll der ST-Autor spezifizieren, welche administrativen Rollen alternative Default-Werte spezifizieren dürfen. Denkbar ist insbesondere der lokale Administrator (siehe auch FMT_SMR.1). Das Security Target kann aber auch ein feineres Rollenmodell spezifizieren.

Erläuterung: FMT_MSA.3/PF erfüllt die Abhängigkeit von FDP_IFF.1/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/PF und FMT_SMR.1) werden in Abschnitt 5.1.1.6 Administration diskutiert.

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

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

Separation von Mehrwertdiensten

Separationsmechanismen für Mehrwertdienste schützen die Sicherheitsfunktionen (TSF), deren Daten (TSF data) und Benutzerdaten (user data) vor möglicherweise schädlichem Einfluss der Mehrwertdienste. WAN-Verbindungen sind nach dem Aufbau der VPN Verbindung nur von und zum VPN-Konzentrator möglich. Ferner sind solche Verbindungen erlaubt, die im Rahmen des Verbindungsaufbaus zum VPN-Konzentrator erforderlich sind (z.B. DNS-Abfragen).

Application Note 77: Direkte Verbindungen zwischen Netzkonnektoren sind nicht vorgesehen.

FPT_SEP.1/VAS	**TSF domain separation**
	Trennung der Sicherheitsfunktionalität von Mehrwertdiensten (value-added services)
Dependencies:	No dependencies.
FPT_SEP.1.1/VAS	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2/VAS	The TSF shall enforce separation between the security domains of subjects in the TSC.
Refinement:	The TOE protects itself from interference of other executable code running on the same abstract machine. The TOE allows WAN connections only to the VPN concentrator that connects care providers (Leistungserbringer) to the central telematics infrastructure (zentrale Telematikinfrastruktur) and optionally to other VPN concentrators used for value-added services (Mehrwertdienste). The TOE **must not** provide direct access to servers and services provided by the transport network (e.g. the Internet), except for those connections that are necessary in order to establish the VPN connections (e.g. DNS queries).

Application Note 78: Der ST-Autor kann anstelle der Anforderung FPT_SEP.1/VAS auch Anforderungen aufnehmen, die hierzu hierarchisch sind (FPT_SEP.2 oder FPT_SEP.3) und wird hier explizit zu einer Prüfung dieser Alternativen ermutigt. Ob dies sinnvoll oder gar erforderlich ist, hängt von der konkreten Ausgestaltung des EVGs ab. Siehe dazu auch die Liste von Separationsmechanismen in Application Note 90: (hinter FPT_AMT.1).

5.1.1.3. Netzdienste

Echtzeituhr und Zeitsynchronisation

Der EVG verfügt über eine eigene Echtzeituhr mit einer zu spezifizierenden Freilaufgenauigkeit (FPT_STM.1/TOE) und führt in regelmäßigen Abständen eine Zeitsynchronisation mit einem zentralen Zeitdienst durch (FPT_TDC.1/Time). Siehe auch Sicherheitsdienst (3) (a) Echtzeituhr/Zeitsynchronisation und Application Note 25:.

FPT_STM.1/TOE	**Reliable time stamps**
	Der EVG verfügt über eine eigene verlässliche Systemzeit (Echtzeituhr).
Dependencies:	No dependencies.
FPT_STM.1.1/TOE	The TSF shall be able to provide reliable time stamps for its own use.
Refinement:	Die Echtzeituhr des EVG hält eine Freilaufgenauigkeit von [assignment: *Angabe der Freilaufgenauigkeit*] ein.

Application Note 79: Der ST-Autor soll die vom EVG eingehaltene Freilaufgenauigkeit spezifizieren *(z.B. in ppm, Sekunden pro Tag oder Sekunden pro Jahr).* Vorgaben diesbezüglich ergeben sich aus der Konnektor-Spezifikation [20] (unter dem Stichwort „Freilaufgenauigkeit“).

FPT_TDC.1/Time	**Inter-TSF basic TSF data consistency**
	Regelmäßiger Abgleich der Systemzeit über Netzverbindungen
Dependencies:	No dependencies.
FPT_TDC.1.1/Time	The TSF shall provide the capability to consistently interpret *system time information*[45] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/Time	The TSF shall use *a maximum allowed deviation [assignment: maximum allowed deviation (e.g. in seconds)] between the network time and the local TOE time*[46] when interpreting the TSF data from another trusted IT product.
Refinement:	Das andere vertrauenswürdige IT-Produkt (another trusted IT product) ist ein Zeitserver in der zentralen Telematikinfrastruktur, der über den oder die VPN-Konzentratoren für Dienste gemäß § 291 a SGB V erreichbar ist. Der EVG muss seine eigene Systemzeit (siehe FPT_STM.1/TOE) auf Basis der Netzwerk-Zeit aktualisieren. Bei zu großer Zeitabweichung zwischen Netzwerk-Zeit und eigener Systemzeit muss der EVG die eigene Systemzeit trotzdem aktualisieren, außerdem soll er in diesem Fall den Administrator warnen. Der EVG muss den Abgleich in regelmäßigen Zeitintervallen (gemessen mit seiner eigenen Echtzeituhr, siehe FPT_STM.1/TOE) initiieren. Die Synchronisation muss über das NTP/SNTP-Protokoll, Version 4, gemäß *The Network Time Protocol (NTP) Version 4 Protocol Specification* [32] bzw. *Simple Network Time Protocol (SNTP)*

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

[46] assignment: *list of interpretation rules to be applied by the TSF*

Version 4 for IPv4, IPv6 and OSI [33] oder einen diesen ablösenden Mechanismus erfolgen.

Application Note 80: Die Prüfung auf eine maximale Zeitabweichung (maximum allowed deviation) und Alarmierung des Administrators bei zu großer Abweichung soll Angriffe zusätzlich erschweren, die Systemzeit durch einen Angreifer massiv zu verändern.

Bei der ersten Synchronisation nach der Erstinbetriebnahme bzw. nach dem manuellen Setzen der Zeit durch einen Administrator (falls der EVG eine solche Funktionalität bietet) kann der EVG aus Gründen der Benutzerfreundlichkeit eine größere Zeitdifferenz tolerieren. Gegebenenfalls soll der ST-Autor das Refinement zu FPT_TDC.1/Time geeignet anpassen.

Application Note 81: Der ST-Autor kann einen sicheren Kanal für die Übertragung der Netzwerk-Zeit fordern (im Sinne FPT_ITC.1). Siehe auch Application Note 25: und Abschnitt 7.6.16.

Erläuterung: Der Zeitserver bezieht seine Zeitinformation von einem Referenz-Zeitstempel, der durch die Umgebung bereitgestellt wird (FPT_STM.1/Env).

Zertifikatsprüfung

Der EVG muss die Gültigkeit der Zertifikate überprüfen, die für den Aufbau des VPN-Kanals verwendet werden. Die Zertifikate werden mathematisch geprüft und mit Sperrlisten (Certificate Revocation Lists, CRLs) abgeglichen. Die Sperrlisten werden vor ihrer Verteilung signiert; der EVG muss diese Signatur prüfen.

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

Prüfung der Gültigkeit von Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/Zert The TSF shall provide the capability to consistently interpret *information about the validity of certificates (Certificate Revocation Lists, CRLs)*[47] when shared between the TSF and another trusted IT product.

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

Refinement: Das andere vertrauenswürdige IT-Produkt (another trusted IT product) ist der Server, welcher die Sperrlisten (CRLs) verteilt. Der EVG muss die Signatur der Sperrliste verifizieren.

Application Note 82: Der ST-Autor soll die *interpretation rules* in FPT_TDC.1.2/Zert geeignet verfeinern; dazu soll er sich an der aktuellen Version der Konnektor-Spezifikation [20] orientieren.

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

[48] assignment: *list of interpretation rules to be applied by the TSF*

5.1.1.4. Stateful Packet Inspection

Der Netzkonnektor kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“ (engl. „Stateful Packet Inspection“ oder auch „Stateful Inspection“ genannt). Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird. Siehe auch Application Note 23:.

Application Note 83: Weitergehende Angriffe gegen die Systemintegrität des Netzkonnektors müssen abgewehrt werden (robuste Implementierung, Resistenz gegen Angriffe wie von AVA_VLA.4 gefordert), aber nicht im Detail erkannt werden (es wird keine komplexe Erkennungslogik für Angriffe gefordert).

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

Der EVG generiert Audit-Daten (FAU_GEN.1/Stateful) für eine Auswertung mit dem Ziel grundlegender Intrusion Prevention (FAU_SAA.1). Eine darüber hinausgehende Auswertung der Audit-Daten kann optional außerhalb des EVG erfolgen (FAU_SAR.1/Env).

FAU_GEN.1/Stateful	**Audit data generation**
	Generierung von Audit-Daten für spätere grundlegende Intrusion Prevention (zustandsgesteuerte Filterung; stateful packet inspection)
Dependencies:	FPT_STM.1 Reliable time stamps
	hier erfüllt durch: FPT_STM.1/TOE
FAU_GEN.1.1/Stateful	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) *Information needed for subsequent basic intrusion prevention.*[49]
FAU_GEN.1.2/Stateful	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

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

Application Note 84: Der EVG muss eine kurze Historie des Verbindungszustands (interner Zustand, state) führen, anhand derer er über die Zulässigkeit von Informationsflüssen (siehe FDP_IFC.1/PF) entscheiden kann (stateful packet inspection; die vom EVG generierten Audit-Daten repräsentieren den „Zustand“ für die zustandsgesteuerte Filterung). Diese Komponente (FAU_GEN.1/Stateful) stellt keine Audit-Funktion im gebräuchlicheren Wortsinne dar; dazu siehe FAU_GEN.1/Audit. Bei der selection in FAU_GEN.1.1/Stateful, Punkt b) (level of audit) wird der ST-Autor üblicherweise die Auswahl „not specified“ treffen.

Die Anforderungen an die Dauer der Speicherung ergeben sich aus der Anforderung, dass stateful packet inspection möglich sein muss. Sobald eine Verbindung abgebrochen wird, können alle mit ihr verbundenen gespeicherten Informationen gelöscht werden.

Application Note 85: Optional kann der ST-Autor auch zusätzlich die Anforderung FAU_SAA.3 (*Simple attack heuristics*) aus CC Teil 2 [2] in das Security Target aufnehmen.

FAU_SAA.1	**Potential violation analysis**
	Grundlegende Intrusion Prevention-Funktionalität
Dependencies:	FAU_GEN.1 Audit data generation
	hier erfüllt durch: FAU_GEN.1/Stateful
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation; b) [assignment: *any other rules*].

Application Note 86: Als Mindestanforderung wird das durch FAU_GEN.1/Stateful generierte Protokoll dazu verwendet, zustandsgesteuerte Filterung und damit grundlegende Intrusion Prevention durchzuführen (FAU_SAA.1). Der ST-Autor soll durch die Operationen in FAU_SAA.1.2 präzisieren, welche Funktionalität genau der EVG bietet.

Eine weitergehende Auswertung des Audit Logs (FAU_SAR.1) kann optional durch die Umgebung erfolgen (siehe FAU_SAR.1/Env). Es ist dem ST-Autor freigestellt, ergänzende Anforderungen (z.B. FAU_SAA.3, FAU_SAR.1, FAU_ARP.1) auch in das Security Target mit aufzunehmen.

5.1.1.5. 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). 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	**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	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[50] the following objects: *cryptographic keys (and session keys) used for the VPN, personal medical data, sensitive user data (zu schützende Daten),* [assignment: *list of objects* (this list may be an empty list)][51].
Refinement:	The sensitive user data shall be overwritten with constant or random values when they are not used any longer. In any case, sensitive user data shall be overwritten at start-up after power-on or after a reset.

Application Note 87: Wann ein Datum nicht mehr benötigt wird und somit aktiv überschrieben werden muss, sollte sinnvoll festgelegt werden; dabei sollten weitere Aspekte wie Performance und Vermeidung unnötig häufiger Schlüsselableitungen berücksichtigt werden. Der Konnektor speichert keine *zu schützenden Daten* (medizinischen Daten) dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z.B. während einer Ver- oder Entschlüsselung).

Selbsttests

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

FPT_TST.1	**TSF testing**
	Selbsttests
Dependencies:	FPT_AMT.1 Abstract machine testing

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

[51] assignment: *list of objects*

hier erfüllt durch: FPT_AMT.1

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF data*].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Refinement: Zur Erfüllung der Anforderungen aus FPT_TST.1 muss der EVG mindestens die Mechanismen implementieren, welche dem aktuellen Stand der Technik bei Einzelplatz-Signaturanwendungs-komponenten entsprechen.

Falls der EVG einen physikalischen Zufallszahlengenerator beinhaltet, muss dessen korrekte Funktionsweise nach dem Start getestet werden (vgl. Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116) [16]).

Application Note 88: Beispiele für die im Refinement geforderten Mechanismen sind:

- Eine Prüfung mit kryptographischen Prüfsummen (Hashwerten) der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (z.B. Konfigurationsdateien, TSF data) beim Programmstart sowie
- die Möglichkeit, einen aussagekräftigeren Test mit einem externen Vertrauensanker manuell anzustoßen (z.B. von CD-ROM ablaufender Test: Die CD-ROM enthält in diesem Fall das Testprogramm und die gültigen Hashwerte bzw. Signaturen).

Application Note 89: Optional kann der EVG physische Sicherheitsmaßnahmen implementieren; siehe auch Application Note 27:. Auch möglich ist die Verwendung eines externen Vertrauensankers (z.B. CD-ROM); siehe dazu auch Application Note 28:.

FPT_AMT.1 Abstract machine testing

Dependencies: No dependencies.

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user,[assignment: other conditions]*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application Note 90: Für den Fall, dass der EVG aus Hardware und Software besteht, ergibt sich eine große Schnittmenge aus den Anforderungen aus FPT_AMT.1 und denen aus FPT_TST.1. Es ist denkbar, dass in diesem Fall beide funktionale Anforderungen durch dieselben Funktionen bzw. Mechanismen umgesetzt werden.

Die *underlying abstract machine* kann aus Hardware oder Hardware und Software (z.B. Betriebssystem) bestehen. Siehe auch Abschnitt 7.6.3 reine Software-Lösung und Abschnitt 7.6.4 Betriebssystem als Bestandteil des EVGs.

Die Art der durchzuführenden Tests kann in diesem Schutzprofil noch nicht festgelegt werden. Hier muss der ST-Autor geeignete Zuweisungen vornehmen. FPT_AMT.1 soll die vom EVG benötigte Sicherheitsfunktionalität der *underlying abstract machine* testen. Es sollten insbesondere die folgenden Aspekte betrachtet werden:

- Sicherer Schlüsselspeicher
- Separationsmechanismen für die Trennung zwischen Netzkonnektor und Anwendungskonnektor, falls beide auf einer gemeinsamen Plattform ablaufen (Einbox-Lösung),
- Separationsmechanismen für die Trennung von Mehrwertdiensten (z.B. bei gleichzeitiger Ausführung nicht evaluierter Mehrwertdienste auf derselben Plattform),
- Separationsmechanismen für den Fall, dass nicht evaluierter ausführbarer Code (z.B. Updates von nicht evaluierten Mehrwertdiensten) nachgeladen werden kann.

Die exakten Anforderungen hängen auch von der genauen Ausformulierung der Annahme A.phys_Schutz im Security Target ab.

Sicherer Schlüsselspeicher

Der EVG bietet einen sicheren Schlüsselspeicher (hier modelliert als Zugriffskontrolle auf die innerhalb des sicheren Schlüsselspeichers befindlichen *user data*, Anforderungen: FDP_ACC.1/KeySt, FDP_ACF.1/KeySt). Der Schlüsselspeicher wird verwendet zur Speicherung von

- Sitzungsschlüsseln (session keys), die abgeleitet werden von auf dem SM-K gespeicherten Geheimnissen (privater Schlüssel) zur Authentisierung beim Aufbau des VPN-Tunnels (kryptographische Identität des Netzkonnektors, siehe FTP_ITC.1/VPN),
- Prüfschlüsseln (z.B. öffentlicher Schlüssel) zur Verifikation der eigenen Integrität,
- Prüfschlüsseln (z.B. öffentlicher Schlüssel) zur Verifikation der Authentizität von Software-Updates, sowie
- optional zur Speicherung von Geheimnissen (z.B. privater Schlüssel) zur Entschlüsselung von Software-Updates, falls diese in verschlüsselter Form übertragen werden.
- Schließlich: Geheimnisse, mit denen der Administrator sich gegenüber dem EVG authentisieren kann (FTP_TRP.1/Admin).

Der sichere Schlüsselspeicher schützt also sowohl die Vertraulichkeit als auch die Integrität des in ihm gespeicherten Schlüsselmaterials.

Bedingt durch die Zugriffskontrolle ergeben sich funktionale Abhängigkeiten hinsichtlich der Voreinstellungen (Default-Werte, FMT_MSA.3/KeySt) und der Verwaltung der Zugriffsrechte (FMT_MSA.1/KeySt) für den sicheren Schlüsselspeicher.

FDP_ACC.1/KeySt	**Subset access control**
	Sicherer Schlüsselspeicher (key storage)
Dependencies:	FDP_ACF.1 Security attribute based access control
	hier erfüllt durch: FDP_ACF.1/KeySt
FDP_ACC.1.1/KeySt	The TSF shall enforce the *key storage SFP (KS SFP)*[52] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Application Note 91: Zum assignment *list of subjects, objects, and operations among subjects and objects covered by the SFP* siehe auch Application Note 92:.

FDP_ACF.1/KeySt	**Security attribute based access control**
	Eigenschaften der Zugriffskontrolle für den sicheren Schlüsselspeicher (key storage)
Dependencies:	FDP_ACC.1 Subset access control
	hier erfüllt durch: FDP_ACC.1/KeySt
	FMT_MSA.3 Static attribute initialisation
	hier erfüllt durch: FMT_MSA.3/KeySt
FDP_ACF.1.1/KeySt	The TSF shall enforce the *key storage SFP (KS SFP)*[53] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
FDP_ACF.1.2/KeySt	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
FDP_ACF.1.3/KeySt	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
FDP_ACF.1.4/KeySt	The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[52] assignment: *access control SFP*

[53] assignment: *access control SFP*

Application Note 92: Die Zugriffskontrolle auf den sicheren Schlüsselspeicher muss sicherstellen, dass dort abgelegte Schlüssel und Geheimnisse nur von autorisierten Benutzern gelesen und verwendet werden können. Technisch ist hier eine Vielzahl von Lösungen denkbar, die dieses Schutzprofil nicht beschränken will. Der ST-Autor soll mit Hilfe der Zuweisungen in dieser Komponente FDP_ACF.1/KeySt beschreiben, wie der Schlüsselspeicher genutzt werden kann. Der ST-Autor soll dabei insbesondere beschreiben, welche Zugriffsrechte es gibt und wie diese vergeben werden. – Siehe dazu auch Application Note 94:.

FMT_MSA.3/KeySt	**Static attribute initialisation**
	Default-Werte für die Zugriffsrechte auf den sicheren Schlüsselspeicher (key storage)
Dependencies:	FMT_MSA.1 Management of security attributes
	hier erfüllt durch: FMT_MSA.1/KeySt
	FMT_SMR.1 Security roles
	hier erfüllt durch: FMT_SMR.1
FMT_MSA.3.1/KeySt	The TSF shall enforce the *key storage SFP (KS SFP)*[54] to provide [selection, choose one of: *restrictive*, *permissive*, [assignment: *other property*]] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/KeySt	The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Application Note 93: Zum assignment *the authorised identified roles* und zu evtl. erforderlichen Anpassungen an FMT_SMR.1 siehe auch Application Note 94:.

FMT_MSA.1/KeySt	**Management of security attributes**
	Verwaltung der Zugriffsrechte auf den sicheren Schlüsselspeicher (key storage)
Dependencies:	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	hier erfüllt durch: FDP_ACC.1/KeySt
	FMT_SMR.1 Security roles
	hier erfüllt durch: FMT_SMR.1
	FMT_SMF.1 Specification of Management Functions

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

hier erfüllt durch: FMT_SMF.1

FMT_MSA.1.1/KeySt The TSF shall enforce the *key storage SFP (KS SFP)*[55] to restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, [assignment: *other operations*]] the security attributes *access rights*, [assignment: *list of additional security attributes* (list may be empty)][56] to [assignment: *the authorised identified roles*].

Application Note 94: Die Verwaltung der Zugriffsrechte auf den sicheren Schlüsselspeicher kann durch den Administrator (FMT_SMR.1) vorgenommen werden oder gemäß der Sicherheitspolitik der Applikationen bestimmt werden. Denkbar ist auch, dass der EVG gar keine Modifikation der Zugriffsrechte auf den sicheren Schlüsselspeicher zulässt und die dort gespeicherten Schlüssel nur von eigenen Sicherheitsfunktionen (TSF) genutzt werden. Der ST-Autor soll im Security Target beschreiben, welche Möglichkeiten zur Administration durch autorisierte Rollen (z.B. authentisierter Administrator) der EVG bietet. Abhängig von den Fähigkeiten des EVG und von der erfolgten Zuweisung zu *the authorised identified roles* muss ggf. FMT_SMR.1 angepasst werden.

Es ist zulässig, neben dem Administrator weitere Rollen zu definieren; deswegen wurden die Rollen noch nicht zugewiesen.

Application Note 95: Optional kann der ST-Autor zusätzlich physischen Schutz für den sicheren Schlüsselspeicher bzw. für den gesamten EVG fordern (etwa mittels FPT_PHP.1 oder FPT_PHP.3). Siehe auch Abschnitt 7.6.3 reine Software-Lösung und Abschnitt 7.6.7.

Schutz von Geheimnissen, Side Channel-Resistenz

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: Sekundäre Werte in Abschnitt 3.1.2) und insbesondere für den privaten Authentisierungsschlüssel für das VPN (FTP_ITC.1/VPN). Zur Definition der Anforderung FPT_EMSEC.1 siehe Abschnitt 6.3.1.

Application Note 96: Falls der EVG eine Funktion zur Entschlüsselung im Rahmen von Software-Updates bietet (siehe FPT_ITI.1/Update und Application Note 111:), dann sollte auch das dafür verwendete Schlüsselmaterial gegen unbefugte Kenntnisnahme geschützt werden; der ST-Autor soll in diesem Fall die Anforderung FPT_EMSEC.1 geeignet anpassen (konkret muss das assignment: *list of types of TSF data* in FPT_EMSEC.1.1 erweitert werden).

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

[56] assignment: *list of security attributes*

FPT_EMSEC.1	**TOE Emanation**
FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to - *session keys derived from private VPN authentication keys,* - *key material used to verify the TOE's integrity (during self tests),* - *key material used to verify the integrity and authenticity of software updates,* - [selection: *none, key material used to decrypt encrypted software updates (if applicable)*], - [selection: *none, key material used for authentication of administrative users (if applicable)*][57], [assignment: *list of other types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.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*].
Dependencies:	No other components.

Application Note 97: Der ST-Autor muss hier geeignete Zuweisungen vornehmen; siehe dazu auch Abschnitt 7.6.17.

Sichere Kommunikation zwischen verteilten Komponenten des EVG

Application Note 98: Im Fall einer Mehrbox-Lösung (siehe auch Application Note 6: und Application Note 30:) kann der ST-Autor hier Anforderungen an eine gesicherte Kommunikation zwischen den Teilen des EVG formulieren (etwa mittels FDP_ITT.1, FPT_ITT.1). Falls die Kommunikation durch organisatorische Maßnahmen geschützt wird (siehe A.phys_Schutz), sind keine funktionalen Sicherheitsanforderungen an den EVG erforderlich.

Optional kann der ST-Autor hier auch sichere Kanäle zu anderen dezentralen Komponenten (z.B. SM-K) fordern (etwa mittels FTP_ITC.1). Denkbar ist auch, dass der EVG über Mechanismen verfügt, mit deren Hilfe er erkennen kann, wenn ein SM-K entfernt wird. Siehe auch Abschnitt 7.6.16.

Ereignisprotokollierung

Der EVG führt ein Ereignisprotokoll wie unter Sicherheitsdienst (5) (f) *Protokollierung* in Abschnitt 2.4 beschrieben. Vergleiche dazu auch die Konnektor-Spezifikation [20], Version 2.0.0, Abschnitt 4.2.3.3 *Protokollierung / Logging*.

[57] assignment: *list of types of TSF data*
Note: The two selections have been added by the PP author as part of the assignment – the last two items of the list shall be optional. For more details please see section 7.6.17.

FAU_GEN.1/Audit	**Audit data generation**
Dependencies:	FPT_STM.1 Reliable time stamps hier erfüllt durch: FPT_STM.1/TOE
FAU_GEN.1.1/Audit	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) power on, shut down and reset of the TOE, hardware failures (e.g. failure of power supply, temperature), resource utilization problems, state of LAN and WAN connections (up / down) establishment of a VPN connection and VPN disconnection, identity of VPN concentrators to which a connection is established, certificate validation errors, other VPN error conditions, software updates (successful and unsuccessful), changes of the TOE configuration.[58]
FAU_GEN.1.2/Audit	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].
Refinement:	Das Ereignisprotokoll muss in einem nicht-flüchtigen Speicher abgelegt werden, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Ereignisprotokoll reservierte Speicher muss hinreichend groß dimensioniert sein.

Application Note 99: Der ST-Autor soll die Liste der zu protokollierenden Ereignisse unter FAU_GEN.1.1/Audit Punkt c) mit der jeweils aktuellen Version der Konnektor-Spezifikation [20] abgleichen und die funktionale Anforderung FAU_GEN.1/Audit geeignet anpassen. Siehe auch Application Note 31:. – Die Auswertung des Ereignisprotokolls erfolgt durch die Umgebung (siehe FAU_SAR.1/Env). – Der Administrator darf die Protokolleinträge nicht löschen können (siehe FAU_STG.1). Der EVG muss bei Konfigurationsänderungen durch authentisierte Administratoren die Identität des ändernden Administrators in das Ereignisprotokoll aufnehmen. Falls der EVG mehrere Administrator-Rollen unterstützt, soll der Audit-Eintrag die jeweilige Administrator-Rolle eindeutig identifizieren.

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

FAU_GEN.2	**User identity association**
Dependencies:	FAU_GEN.1 Audit data generation
	hier erfüllt durch: FAU_GEN.1/Audit
	FIA_UID.1 Timing of identification
	hier erfüllt durch: FIA_UID.1/SMR
FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note 100: Der EVG muss bei Konfigurationsänderungen durch authentisierte Administratoren die Identität des ändernden Administrators in das Ereignisprotokoll aufnehmen. Falls der EVG mehrere Administrator-Rollen unterstützt, soll der Audit-Eintrag die jeweilige Administrator-Rolle eindeutig identifizieren.

FAU_STG.1	**Protected audit trail storage**
Dependencies:	FAU_GEN.1 Audit data generation
	hier erfüllt durch: FAU_GEN.1/Audit
FAU_STG.1.1	The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to *prevent*[59] unauthorised modifications to the stored audit records in the audit trail.

Application Note 101: Niemand darf die durch FAU_GEN.1/Audit erzeugten Audit-Daten verändern oder löschen – die Daten werden automatisch vom EVG selbst zyklisch überschrieben. Da der EVG selbst autorisiert ist, die Daten zyklisch zu überschreiben, gibt es ein Löschen von Daten – aber unautorisiertes Überschreiben soll verhindert werden.

FAU_STG.3	**Action in case of possible audit data loss**
Dependencies:	FAU_STG.1 Protected audit trail storage
	hier erfüllt durch: FAU_STG.1
FAU_STG.3.1	The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

[59] selection, choose one of: *prevent, detect*

Application Note 102: Wie in der Konnektor-Spezifikation [20], Abschnitt 4.2.3.3, beschrieben soll der Konnektor ein Event Log zur Betriebsführung (als Hilfe zur Fehlersuche und Administration, in diesem Schutzprofil nicht näher beschrieben) und ein Sicherheits-Log (Security Log, vgl. FAU_GEN.1/Audit) unterscheiden; nur letzteres stellt eine Sicherheitsfunktionalität dar. Wenn der für die Protokolleinträge vorgesehene Speicherbereich verbraucht ist, muss der EVG alte Einträge zyklisch überschreiben.

5.1.1.6. Administration

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

Der EVG verwaltet mindestens eine Administrator-Rolle (FMT_SMR.1). Der Administrator muss sich authentisieren (FIA_UID.1/SMR und FIA_UAU.1/SMR), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1).

Die Wartung selbst erfolgt immer dann, wenn der Administrator über Netzwerkverbindungen (z.B. LAN) zugreift, über einen sicheren Pfad (FTP_TRP.1/Admin). Falls der lokale Administrator die Wartung über eine dedizierte physische Schnittstelle (PS3) durchführt, kann auf die Anforderung eines gesicherten Pfads für ihn verzichtet werden, andernfalls (bei Verwendung der LAN-Schnittstelle PS1) muss der Administrationspfad abgesichert werden (siehe Application Note 107:).

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

FMT_SMR.1	**Security roles**
Bemerkung:	Der EVG unterstützt die Rolle Administrator.
Dependencies:	FIA_UID.1 Timing of identification hier erfüllt durch: FIA_UID.1/SMR
FMT_SMR.1.1	The TSF shall maintain the roles • *Administrator*[60].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Bemerkung:	Neben der Identifikation (FIA_UID.1/SMR) wird auch eine Authentisierung gefordert, siehe FIA_UAU.1/SMR.
Refinement:	Der EVG muss vor jeder administrativen Tätigkeit (durch einen Administrator) eine Benutzeridentifikation und –authentisierung dieses Administrators erzwingen (siehe FIA_UID.1/SMR und FIA_UAU.1/SMR sowie FMT_MTD.1 und FAU_STG.1).

[60] assignment: *the authorised identified roles*

Application Note 103: Externe vertrauenswürdige IT-Systeme wie der Anwendungskonnektor oder Kartenterminals sind keine Rollen, also ohne Einfluss auf FMT_SMR.1. Der ST-Autor wird bereits in Application Note 30: darauf hingewiesen, dass im Falle einer Mehrbox-Lösung gegebenenfalls zusätzliche sichere Kanäle (FTP_ITC.1) zu etablieren sind.

FMT_MTD.1	**Management of TSF data**
	Nur Administratoren dürfen administrieren: Die aufgelisteten administrativen Tätigkeiten können nur von Administratoren ausgeführt werden.
Dependencies:	FMT_SMR.1 Security roles
	hier erfüllt durch: FMT_SMR.1
	FMT_SMF.1 Specification of Management Functions
	hier erfüllt durch: FMT_SMF.1
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clear*, *perform*[61], [assignment: *other operations*]] the *system clock, secure software update* [assignment: *list of other TSF data* (may be empty)][62] to *the role Administrator*[63].

Application Note 104: Die *system clock* bezieht sich auf die von FPT_STM.1/TOE geforderte Echtzeituhr. Das *secure software update* wird durch FPT_ITI.1/Update und FPT_RCV.4/Update näher beschrieben; ein solches Update darf nur von einem Administrator durchgeführt werden (*perform*).

FIA_UID.1/SMR	**Timing of identification**
	Identification of Security Management Roles
Dependencies:	No dependencies.
FIA_UID.1.1/SMR	The TSF shall allow *the following TSF-mediated actions:*
	• *all actions except for administrative actions (as specified by FMT_SMF.1, see below)*[64]
	on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/SMR	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

61 [assignment: *other operations*] → *perform*, [assignment: *other operations*]

62 assignment: *list of TSF data*

63 assignment: *the authorised identified roles*

64 assignment: *list of TSF-mediated actions*

Application Note 105: Der ST-Autor darf die Zuweisung *all actions except for administrative actions (as specified by FMT_SMF.1)* im Sinne eines Refinement verändern, d.h., er darf im Security Target eine weniger umfangreiche Menge von Aktionen (*TSF-mediated actions*) anstelle der hier vorgenommenen Auswahl zuweisen. Vor administrativen Tätigkeiten muss die Identifikation verpflichtend bleiben. Gleiches gilt für FIA_UAU.1/SMR (siehe unten).

FIA_UAU.1/SMR	**Timing of authentication**
	Authentication of Security Management Roles
Dependencies:	FIA_UID.1 Timing of identification
	hier erfüllt durch: FIA_UID.1/SMR
FIA_UAU.1.1/SMR	The TSF shall allow *the following TSF-mediated actions* • *all actions except for administrative actions (as specified by FMT_SMF.1, see below)*[65] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/SMR	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 106: Wenn die Authentisierung des Administrators durch Benutzernamen und Passwort erfolgt, soll der EVG einen Fehlbedienungszähler implementieren (z.B. gemäß Anforderung FIA_AFL.1) und den Administrator bei dessen erster Anmeldung zwingen, das Passwort zu ändern, so dass es sich anschließend von einem eventuell voreingestellten (Default-)Passwort unterscheidet.

FTP_TRP.1/Admin	**Trusted path**
	Trusted Path für den Administrator
Dependencies:	No dependencies.
FTP_TRP.1.1/Admin	The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/Admin	The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.
FTP_TRP.1.3/Admin	The TSF shall require the use of the trusted path for *initial user authentication and administrative actions.*[66]

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

Application Note 107: Der ST-Autor kann sich durch die Selection remote / local aussuchen, ob die Wartung über die LAN-Schnittstelle (PS1) und/oder über die WAN-Schnittstelle (PS2) erfolgen kann. Abhängig davon, wie der EVG gewartet wird, soll der ST-Autor die Selection vornehmen.

FMT_SMF.1 **Specification of Management Functions**

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:[67]

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

- Management of access rights to the secure key storage (as required for FDP_ACC.1/KeySt, FDP_ACF.1/KeySt, FMT_MSA.3/KeySt, and FMT_MSA.1/KeySt).

  (Verwalten der Zugriffsrechte auf den sicheren Schlüsselspeicher.)

- Activation and deactivation of the VPN connection (see FMT_MOF.1)

  (Aktivieren und Deaktivieren der VPN-Verbindung zum VPN-Konzentrator)

- Activation and deactivation of the audit log (FAU_GEN.1/Stateful, FAU_GEN.1/Audit).

  (Aktivieren und Deaktivieren der Protokollierungsfunktion)

- Secure Software Update (FPT_ITI.1/Update, FPT_RCV.4/Update).

  (Sicheres Software-Update)

- Reviewing the Audit Log generated by FAU_GEN.1/Audit and by FAU_GEN.1/Stateful

  (Lesen und Auswerten der von FAU_GEN.1/Audit und FAU_GEN.1/Stateful erzeugten Audit-Daten)

---

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

67 assignment: *list of security management functions to be provided by the TSF*

Application Note 108: Das Durchführen gewisser administrativer Aufgaben ist nur den Administratoren erlaubt, siehe FMT_MTD.1.

FMT_MSA.1/PF	**Management of security attributes**
	Nur der Administrator darf die Filterregeln verändern.
Dependencies:	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	hier erfüllt durch: FDP_IFC.1/PF
	FMT_SMR.1 Security roles
	hier erfüllt durch: FMT_SMR.1
	FMT_SMF.1 Specification of Management Functions
	hier erfüllt durch: FMT_SMF.1
FMT_MSA.1.1/PF	The TSF shall enforce the *PF SFP*[68] to restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, [assignment: *other operations*]] the security attributes *packet filtering rules*[69] to *the roles „Administrator“*[70].
Erläuterung:	FMT_MSA.1/PF sorgt als von FMT_MSA.3/PF abhängige Komponente dafür, dass die Regeln für den dynamischen Paketfilter (*packet filtering rules*, diese Regeln werden als security attributes angesehen) nur durch den Administrator (siehe FMT_SMR.1) verändert werden können.

Sicheres Software-Update (*secure software update*)

Der EVG erlaubt eine gesicherte Aktualisierung seiner Firmware und Software. Updates müssen offline eingespielt werden können, d.h., unter Kontrolle eines lokalen Administrators. Optional können Updates auch online eingespielt werden.

Das Update umfasst einen sicheren Download von Updates und deren automatische Integritätsprüfung und Aktivierung. Die Integrität des Updates wird durch FPT_ITI.1/Update gefordert. Optional kann auch die Vertraulichkeit gefordert werden, siehe Application Note 111:.

Falls während des Software-Updates ein Fehler auftritt, muss der EVG seine Betriebsfähigkeit wiederherstellen (FPT_RCV.4/Update) – etwa indem auf die letzte gültige Software-Version zurückgefallen wird.

---

68 assignment: *access control SFP, information flow control SFP*

69 assignment: *list of security attributes*

70 assignment: *the authorised identified roles*

FPT_ITI.1/Update	**TSF detection of modification of received TSF-data**[71]
	Schutz der Datenintegrität von Software-Updates (als Teil der Funktionalität *secure software update*)
Dependencies:	No dependencies.
FPT_ITI.1.1/Update	The TSF shall provide the capability to detect modification of all TSF data during transmission *of a secure software update*[72] between *a remote trusted IT product and the TSF*[73] within the following metric: *an electronic signature created over the software update*[74].
FPT_ITI.1.2/Update	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between *a remote trusted IT product and the TSF*[75] and perform [assignment: *action to be taken*] if modifications are detected.
Refinement:	Das *remote trusted IT product* ist der Dienst, welcher Software-Updates verteilt.

Application Note 109: Diese Anforderung soll ein sicheres Software-Update ermöglichen. Eine ausführliche Erläuterung zur Auswahl und Verfeinerung der Komponente FPT_ITI.1 findet sich in Abschnitt 7.6.18.

Application Note 110: Falls das Update lokal eingespielt wird (z.B. von CD), wird der Herausgeber der CD, der das Update signiert hat, als *remote trusted IT product* angesehen.

Falls der EVG Updates automatisch, das heißt ohne Intervention des Administrators, einspielen kann, wird der ST-Autor ermutigt, einen Fehlbedienungszähler für nicht erfolgreiche Software-Updates einzuführen, der nach einer gewissen Anzahl von fehlgeschlagenen automatischen Updates (z.B. weil die Signatur nicht erfolgreich verifiziert werden konnte oder das Update nicht aktiviert werden konnte) eine manuelle Intervention des Administrators erfordert.

Application Note 111: **Optional** kann der ST-Autor bestimmen, dass der Kanal auch die **Vertraulichkeit** der Nutzdaten für das Software-Update schützt. Auf diese Weise würde es Angreifern erschwert, Informationen über die Interna des EVG zu erlangen. In diesem Fall beinhaltet die Funktionalität Software-Update auch die erforderliche Entschlüsselung. Es steht dem ST-Autor frei, in einem solchen Fall weitere Anforderungen zu ergänzen (z.B. FCS_COP.1/Decrypt oder eine Anforderung analog zu FPT_ITC.1).

---

71 refinement: Inter-TSF detection of modification → TSF detection of modification of received TSF-data

72 refinement: transmission → transmission of a secure software update

73 refinement: the TSF and a remote trusted IT product → a remote trusted IT product and the TSF

74 assignment: *a defined modification metric*

75 refinement: the TSF and a remote trusted IT product → a remote trusted IT product and the TSF

Es ist in der Konnektor-Spezifikation [20] technisch nicht vorgesehen, dass der Update-Server verfügbare Updates im Push-Verfahren an die EVGs verteilt, sondern jeder EVG muss stets selbst aktiv nach Updates fragen (Polling-Verfahren). Dabei gibt es aber noch den qualitativen Unterschied, ob jedes verfügbare und durch Polling gefundene Update stets automatisch vom EVG installiert wird, oder ob ein Administrator diese Entscheidung treffen und ggf. auch Updates ablehnen oder verzögert einspielen kann. Der ST-Autor soll im Security Target beschreiben, wie sich der EVG diesbezüglich verhält bzw. ob und ggf. wie das Verhalten konfiguriert werden.

Siehe auch Application Note 34:.

Application Note 112: Es ist denkbar, dass Software-Updates technisch mit einem **Hybrid-Verfahren** verteilt werden, welches sowohl symmetrische als auch asymmetrische Kryptoalgorithmen als Mechanismen verwendet. Es steht dem ST-Autor frei, abhängig von der im konkreten Produkt verwendeten Lösung spezifischere Anforderungen zu formulieren (z.B. mittels FCS_COP.1 die zu verwendenden symmetrischen und asymmetrischen Algorithmen festzulegen). Dabei sind die Vorgaben aus der Konnektor-Spezifikation [20] zu beachten; siehe auch Application Note 115: Kryptokonzept.

Application Note 113: Der ST-Autor kann **optional** auch fordern, dass zusätzlich zur Authentisierung des Absenders (implizit durch die Prüfung der Datenintegrität und -authentizität, z.B. durch eine Signatur über das Software-Update) auch eine **Authentisierung des EVGs** erfolgen soll. Auf diese Weise könnte der zentrale Dienst, welcher Software-Updates verteilt, stets darüber informiert bleiben, welche im Feld installierten Konnektoren über welche Software-Versionsstände verfügen. Vor diesem Hintergrund ist es dem ST-Autor freigestellt, die Anforderung nach einem *Trusted Channel* (FTP_ITC.1) zu ergänzen. Die Kommunikation mit dem Update-Server **sollte** über einen sicheren Kanal erfolgen, beispielsweise gesichert durch FTP_ITC.1/VPN.

FPT_RCV.4/Update	**Function recovery**
	Sequenzkontrolle für sicheres Software-Update (als Teil der Funktionalität *secure software update*)
Dependencies:	ADV_SPM.1 Informal TOE security policy model
	hier erfüllt durch: ADV_SPM.1 (Teil von EAL4)
FPT_RCV.4.1/Update	The TSF shall ensure that *the security functionality (SF) secure software update (with the failure scenarios listed below)*[76] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state. *This shall be valid for the following failure scenarios:* • *Data integrity and authenticity of the software update cannot be verified successfully (integrity error),* • *the new software cannot be installed and/or activated successfully (e.g. due to some technical error).*

[76] assignment: *list of SFs and failure scenarios*

Refinement: Der Wiederherstellung (recovery) eines sicheren Zustands (*consistent and secure state*) besteht darin, dass der EVG, falls möglich, die letzte gültige Software-Version reaktiviert (und gegebenenfalls neu startet). Sollte dies nicht mehr möglich sein, muss der EVG in einen sicheren Fehlerzustand übergehen. In jedem Fall muss ein definierter Wiederaufsetzpunkt erreicht werden.

Application Note 114: Das Software-Update muss durch eine Sequenzkontrolle gesteuert werden, welche verhindert, dass der EVG in einen unsicheren Zustand gelangt. Der aktualisierte Software-Stand darf erst dann aktiviert werden, wenn seine Integrität und Authentizität erfolgreich überprüft werden konnte, und die aktualisierte Software darf erst dann gestartet werden, wenn sie vollständig und korrekt installiert wurde.

Der sichere Fehlerzustand könnte beispielsweise darin bestehen, dass der EVG in einen Wartungsmodus übergeht, der nur durch ein erneutes, erfolgreiches Software-Update oder durch manuelle Intervention eines Administrators verlassen werden kann. Die Intervention des Administrator könnte z.B. im Aufspielen eines gültigen Software-Updates über eine lokale Wartungsschnittstelle bestehen. Während der EVG sich im Wartungsmodus befindet, muss er die Aufnahme des normalen (operationalen) Wirkbetriebs verweigern.

5.1.1.7. Kryptographische Basisdienste

Der Konnektor soll laut Spezifikation [20] (Version 2.0.0, Abschnitt 4.1.2 *Basismechanismen* und Unterabschnitte) die im Folgenden aufgelisteten kryptographischen Primitive implementieren.

Application Note 115: **Kryptokonzept:** Die konkreten Mechanismen sollen in diesem Schutzprofil nicht explizit benannt werden, sondern es wird stattdessen auf die zu diesem Zweck erstellten und gepflegten Dokumente verwiesen:

- Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116) [16],
- Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpecKrypt] [22] und
- Konnektorspezifikation [gemSpec Kon] [20].

Die Dokumente in obiger Liste sind nach aufsteigendem Präzisierungsgrad gelistet.

Zufallszahlen können von einem qualitativ hochwertigen Zufallszahlengenerator aus der IT-Einsatzumgebung bezogen werden (siehe OE.RNG sowie FCS_RND.1/Env in Abschnitt 5.2.1).

FCS_COP.1/Hash 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/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. FMT_MSA.2 Secure security attributes hier erfüllt durch: FMT_MSA.2
FCS_COP.1.1/Hash	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 116: Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit den in Application Note 115: Kryptokonzept genannten Dokumenten vornehmen.

Application Note 117: Der EVG kann Zufallszahlen selbst generieren oder diese von einem evaluierten Zufallszahlengenerator (z.B. auf dem SM-K) beziehen. Falls der EVG selbst erzeugte Zufallszahlen nutzt, soll der ST-Autor eine entsprechende Anforderung in das Security Target aufnehmen (z.B. FCS_RND.1 wie in [13], Abschnitt 5.1, definiert). Siehe auch Application Note 126:.

FCS_COP.1/Auth	**Zu unterstützende Authentisierungs-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: FDP_ITC.1/COP FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4 FMT_MSA.2 Secure security attributes hier erfüllt durch: FMT_MSA.2
FCS_COP.1.1/Auth	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 118: Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit den in Application Note 115: Kryptokonzept genannten Dokumenten vornehmen.

FCS_COP.1/Encrypt	**Zu unterstützende Verschlüsselungs-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: FDP_ITC.1/COP FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4 FMT_MSA.2 Secure security attributes hier erfüllt durch: FMT_MSA.2
FCS_COP.1.1/Encrypt	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 119: Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit den in Application Note 115: Kryptokonzept genannten Dokumenten vornehmen.

FCS_COP.1/KeyExch	**Zu unterstützende Schlüsselaustausch-Algorithmen**
	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: FDP_ITC.1/COP FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4 FMT_MSA.2 Secure security attributes hier erfüllt durch: FMT_MSA.2
FCS_COP.1.1/KeyExch	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes

[assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 120: Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit den in Application Note 115: Kryptokonzept genannten Dokumenten vornehmen.

FCS_COP.1/Sign	**Zu unterstützende Signatur-Algorithmen**
	Signatur-Algorithmen, die im Rahmen von Authentisierungsprotokollen oder im Rahmen der Integritätsprüfung von Software-Updates zum Einsatz kommen dürfen
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: FDP_ITC.1/COP
	FCS_CKM.4 Cryptographic key destruction
	hier erfüllt durch: FCS_CKM.4
	FMT_MSA.2 Secure security attributes
	hier erfüllt durch: FMT_MSA.2
FCS_COP.1.1/Sign	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 121: Der ST-Autor soll die Zuweisungen der Operationen im Einklang mit den in Application Note 115: Kryptokonzept genannten Dokumenten vornehmen.

FCS_CKM.4	**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: FDP_ITC.1/COP
	FMT_MSA.2 Secure security attributes
	hier erfüllt durch: FMT_MSA.2

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

Application Note 122: FCS_CKM.4 zerstört die von den Komponenten FCS_COP.1/... (FCS_COP.1/Auth, FCS_COP.1/Encrypt, FCS_COP.1/KeyExch, FCS_COP.1/Sign) benötigten Schlüssel. Der ST-Autor soll spezifizieren, wie die Schlüssel zerstört werden. Das Überschreiben der Schlüssel mit festen oder zufälligen Werten kann ein zulässiges Verfahren darstellen.

FMT_MSA.2 Secure security attributes

Sichere Sicherheitsattribute (bei kryptographischen Berechnungen gemäß FCS_COP.1/...)

Dependencies: ADV_SPM.1 Informal TOE security policy model

hier erfüllt durch: ADV_SPM.1 (Teil der Stufe EAL4)

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_ACC.1/KeySt

FMT_MSA.1 Management of security attributes

hier erfüllt durch: FMT_MSA.1/KeySt

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Application Note 123: Sofern die Ausführung kryptographischer Algorithmen durch Sicherheitsattribute beeinflusst werden kann, darf der EVG nur sichere Werte für die Sicherheitsattribute zulassen.

Beispielsweise muss der EVG verhindern, dass aufgrund eines Bedienfehlers anstelle eines 3DES ein einfacher DES gerechnet werden kann. Sofern zusätzliche Schutzmaßnahmen parametrisiert werden können (etwa doppelte Berechnung als Schutz gegen Angriffe mittels Fehlerinduktion), soll der EVG sicherstellen, dass für die Sicherheit erforderliche Schutzmaßnahmen nicht versehentlich deaktiviert werden.

FDP_ITC.1/COP Import of user data without security attributes

Import von Schlüsselmaterial für diverse FCS_COP.1/... (FCS_COP.1/Auth, FCS_COP.1/Encrypt, FCS_COP.1/KeyExch, FCS_COP.1/Sign)

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_ACC.1/KeySt (siehe dazu die Ausführungen hinter dem Stichwort *Erläuterung* unten)

FMT_MSA.3 Static attribute initialisation

hier erfüllt durch: FMT_MSA.3/KeySt (siehe dazu die Ausführungen hinter dem Stichwort *Erläuterung* unten)

FDP_ITC.1.1/COP The TSF shall enforce the *key storage SFP (KS SFP)*[77] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3/COP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].

Erläuterung: Die Anforderung FDP_ITC.1/COP beschreibt, dass Schlüssel importiert werden. Die importierten Schlüssel werden später von den verschiedenen kryptographischen Operationen (siehe die verschiedenen Anforderungen FCS_COP.1/...) genutzt. Da es sich bei den Schüsseln um schützenswerte Daten handelt, schreibt FDP_ITC.1/COP über eine Abhängigkeit vor, dass die Schlüssel nach dem Import geschützt werden müssen (formalisiert entweder als Zugriffskontrolle oder als Informationsflusskontrolle). Die in FDP_ACC.1/KeySt leistet genau dies: Die dort definierte *key storage SFP (KS SFP)* beschreibt, wie der Zugriff auf die im sicheren Schlüsselspeicher gespeicherten Schlüssel beschränkt wird. Daher erfüllt FDP_ACC.1/KeySt die Abhängigkeit zu [FDP_ACC.1 oder FDP_IFC.1] von FDP_ITC.1/COP.

In ähnlicher Weise fordert eine Abhängigkeit von FDP_ITC.1/COP zu FMT_MSA.3 dazu auf, dass eine Zuweisung von Default-Werten für die Sicherheitsattribute erfolgt, zumal FDP_ITC.1 einen Import ohne Sicherheitsattribute beschreibt – die Sicherheits-attribute müssen also vom EVG gesetzt werden. Die Anforderung FMT_MSA.3/KeySt leistet genau dies, so dass die Abhängigkeit erfüllt wird.

Application Note 124: Für alle mittels FCS_COP.1/... beschriebenen kryptographische Operationen (mit Ausnahme der Hashwert-Berechnung, siehe FCS_COP.1/Hash) sind kryptographische Schlüssel erforderlich, die entsprechend der Abhängigkeiten von FCS_COP.1 aus CC Teil 2 [2] entweder durch eine Schlüsselgenerierung oder durch einen Schlüsselimport zu erfüllen sind. In diesem Schutzprofil wurde ein Schlüsselimport (FDP_ITC.1/COP) gewählt, da der Import von Schlüsseln nach heutigem Kenntnisstand als wahrscheinlichste Lösung angesehen wird.

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

Der EVG darf auch selbst geeignete Schlüssel generieren. Die Schlüsselgenerierung kann sich auf einen, einige oder alle kryptographischen Algorithmen (FCS_COP.1/...) beziehen. Für jeden Schlüssel, den der EVG selbst generieren soll, soll der ST-Autor eine Anforderung FCS_CKM.1 (Cryptographic key generation) in das Security Target aufnehmen; bei Bedarf ist diese Komponente zu iterieren. Wenn der EVG alle erforderlichen Schlüssel selbst generierte, könnte auf die Anforderung FDP_ITC.1/COP vollständig verzichtet werden. Dies erscheint jedoch relativ unrealistisch, da z.B. für den Aufbau des VPN-Kanals (FTP_ITC.1/VPN) Schlüssel zwischen dem VPN-Konzentrator und dem EVG (Netzkonnektor) ausgetauscht werden müssen, was einen Schlüsselimport als wahrscheinlichste Lösung nahe legt (das Zertifikat mit dem Public Key des VPN-Konzentrators wird in den Netzkonnektor importiert, damit der Netzkonnektor den VPN-Konzentrator authentisieren kann).

5.1.2. Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

Es wird die Vertrauenswürdigkeitsstufe EAL4+ (EAL4 erweitert um die Komponenten ADV_IMP.2, AVA_MSU.3 und AVA_VLA.4 gefordert. Daraus ergibt sich eine Stärke der Funktionen „hoch“ im Sinne von AVA_SOF.1.

Die Anforderungen an die Vertrauenswürdigkeit (Assurance) werden wie folgt verfeinert:

Refinement	zu ADV_SPM.1: FPT_RCV.4/Update erzeugt eine Abhängigkeit zu ADV_SPM.1. Das informelle Security Policy Model muss daher beschreiben, wie der konsistente und sichere Zustand (*consistent and secure state*) aussieht, auf den der EVG zurückfallen soll (recovery), wenn während des Software-Updates ein Fehler auftritt.
Refinement	zu ADO_DEL.2: Das Auslieferungsverfahren muss Schutz gegen das In-Umlauf-Bringen gefälschter Konnektoren bieten (sowohl während der Erstauslieferung als auch bedingt durch unbemerkten Austausch), siehe O.TOE_Authenticity. Dies unterstützt die Verwendung der (in EAL4 bereits enthaltenen) Komponente ADO_DEL.2. Das Auslieferungsverfahren muss so ausgestaltet werden, dass das Ziel O.TOE_Authenticity erfüllt wird.
Refinement	zu ADO_IGS.1: 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.TOE_Authenticity. Dies unterstützt die Verwendung der (in EAL4 bereits enthaltenen) Komponente ADO_IGS.1. Das Verfahren zur Inbetriebnahme muss so ausgestaltet werden, dass das Ziel O.TOE_Authenticity erfüllt wird.
Refinement	zu AGD_ADM.1: Die Administratordokumentation muss den Administrator befähigen, einen geeigneten Satz von Paketfilter-Regeln

aufzustellen bzw. die voreingestellten Regeln nur in einer Art und Weise zu modifizieren, welche die Sicherheit des EVG nicht beeinträchtigt. Folgende Aspekte müssen dabei berücksichtigt werden:
a) Alle nicht explizit erlaubten Verbindungen müssen automatisch verboten werden.
b) Für *zu schützende Daten* muss die Verwendung des VPN-Kanals vorgeschrieben werden (siehe auch Abschnitt 5.1.1.1, Unterabschnitt Informationsflusskontrolle).

Application Note 125: Der ST-Autor kann jederzeit weitere Anforderungen an die Vertrauenswürdigkeit aus Teil 3 der Common Criteria [3] aufnehmen. Der ST-Autor wird insbesondere auf die Komponente ALC_FLR.1 *flaw remediation* hingewiesen, deren freiwillige Aufnahme sinnvoll erscheint.

5.2. Sicherheitsanforderungen an die IT-Umgebung

Folgende Sicherheitsanforderungen werden nicht durch den EVG selbst erfüllt, sondern müssen von seiner IT-Einsatzumgebung (IT environment) geleistet werden.

Um diese Sicherheitsanforderung an die IT-Umgebung von der Anforderung an den EVG leicht unterscheiden zu können, wurde diese Sicherheitsanforderungen an die IT-Umgebung durch das Suffix „/Env“ (wie *environment*) gekennzeichnet.

5.2.1. Externer Zufallszahlengenerator

Der Konnektor muss auf einen externen Zufallszahlengenerator zugreifen können, der ihm Zufallszahlen hinreichender Güte liefert. Dazu muss dieser externe Zufallszahlengenerator die explizit definierte Anforderung **FCS_RND.1/Env** erfüllen. Diese Anforderung (FCS_RND.1) wird in Abschnitt 6.3.2 definiert.

Application Note 126: Falls der Konnektor selbst über einen geeigneten Zufallszahlengenerator verfügt, entfällt diese Anforderung an die IT-Umgebung. Der ST-Autor soll aber in diesem Fall eine entsprechende Anforderung (FCS_RND.1) ins Security Target aufnehmen. Siehe auch Application Note 117:.

FCS_RND.1/Env	**Quality metric for random numbers**
Dependencies:	No dependencies.
FCS_RND.1.1/Env	The *IT environment*[78] shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Application Note 127: Die Operation wurde bewusst nicht ausgeführt – der ST-Autor soll abhängig von der Verwendung des Zufallszahlengenerators seine Anforderungen spezifizieren können. Der ST-Autor kann sich dabei an den in Application Note 115: Kryptokonzept aufgelisteten Dokumenten orientieren.

[78] refinement: TSF → IT environment

5.2.2. Zeitserver

Der EVG unterstützt eine Synchronisation seiner Systemzeit mit einem netzbasierten Zeitserver (siehe FPT_TDC.1/Time). Dazu muss der Zeitserver ebenfalls über einen sicheren Zeitstempel verfügen (FPT_STM.1/Env).

FPT_STM.1/Env	**Reliable time stamps**
Dependencies:	No dependencies.
FPT_STM.1.1/Env	The *IT environment*[79] shall be able to provide reliable time stamps for its own use.

5.2.3. Auswertung des Ereignisprotokolls

Die IT-Einsatzumgebung des EVG muss eine Auswertung des vom EVG erzeugten Ereignisprotokolls (siehe FAU_GEN.1/Audit) ermöglichen. Siehe auch Application Note 32:.

Application Note 128: Der ST-Autor kann optional fordern, dass auch die durch FAU_GEN.1/Stateful generierten Audit-Daten durch ein System außerhalb des EVG (in seiner IT-Einsatzumgebung) ausgewertet werden. Falls dies gewünscht ist, soll der ST-Autor die Anforderung FAU_SAR.1/Env geeignet formulieren bzw. verfeinern.

FAU_SAR.1/Env	**Audit review**
Dependencies:	FAU_GEN.1 Audit data generation hier erfüllt durch: FAU_GEN.1/Audit, (optional auch durch: FAU_GEN.1/Stateful)
FAU_SAR.1.1/Env	The TSF shall provide *all users*[80] with the capability to read *audit data generated by FAU_GEN.1/Audit* [assignment: *list of additional audit information (may be empty)*][81] from the audit records.
FAU_SAR.1.2/Env	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.4. LAN-seitiger Paketfilter

Die IT-Einsatzumgebung muss einen LAN-seitigen Paketfilter bereitstellen, welcher den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt.

---

79 refinement: TSF → IT environment

80 assignment: *authorised users*

81 assignment: *list of audit information*

FDP_IFC.1/Env	**Subset information flow control**
	LAN-seitiger Paketfilter
Dependencies:	FDP_IFF.1 Simple security attributes
	Diese Abhängigkeit wird nicht erfüllt. Begründung: Es handelt sich um eine Anforderung an die IT-Einsatzumgebung.
FDP_IFC.1.1/Env	The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].
Refinement:	Die IT-Einsatzumgebung soll einen LAN-seitigen dynamischen Paketfilter bereitstellen, welcher den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützt.

Application Note 129: Im Fall einer Einbox-Lösung wird aus dieser Anforderung an die IT-Einsatzumgebung eine Anforderung an den EVG. Im Fall einer Einbox-Lösung muss der ST-Autor daher die Anforderung FDP_IFC.1/Env (genauer: den gesamten Abschnitt 5.2.4) entfernen, da der EVG (Netzkonnektor) den Schutz des Anwendungskonnektors vor potentiellen Angriffen aus dem LAN bereits durch sein Ziel O.PF_LAN abdeckt, siehe Abschnitt 7.6.19. Der ST-Autor muss alle Hinweise aus Abschnitt 7.6.19 befolgen.

Im Fall einer Mehrkomponentenlösung kann der ST-Autor auf Wunsch die Anforderung FDP_IFC.1/Env weiter präzisieren; als Anregung sei dazu auf FDP_IFC.1/PF und FDP_IFF.1/PF in Abschnitt 5.1.1.2 verwiesen.

6. Erklärungsteil (Rationale)

6.1. Erklärung der Sicherheitsziele (Security Objectives Rationale)

6.1.1. Überblick: Abbildung der Bedrohungen und Annahmen auf Ziele

Die folgende Tabelle 5 bildet die Bedrohungen (Threats) und Annahmen (Assumptions) auf Sicherheitsziele für den EVG und die Umgebung ab.

	Sicherheitsziel für den EVG (O. ...) bzw. für die Umgebung (OE. ...)																								
Bedrohung (T. ...) bzw. Annahme (A. ...)	O.Schutz	O.TOE_Authenticity	O.Admin_EVG	O.Protokoll	O.Update	O.Zeit	O.VPN_Auth	O.Zert_Prüf	O.VPN_Vertraul	O.VPN_Integrität	O.PF_WAN	O.PF_LAN	O.Stateful	OE.PKI	OE.RNG	OE.SM-K	OE.Zeitsynchro	OE.AK	OE.phys_Schutz	OE.PF_LAN	OE.sichere_TI	OE.kein_DoS	OE.Betrieb_AK	OE.Admin_EVG	OE.Update	OE.Ersatzverfahren
T.local_TOE_LAN	X			X								X	(x)							X						
T.remote_TOE_WAN	X			X		X	X	X		X	X		X	X	X	X	X				X					
T.remote_TOE_LAN	X			X		X	X	X		X	X	X	(x)	X	X	X	X			X	X					
T.remote_VPN_Data				(x)		X	X	X	X	X				X	X	X	X	X			X		X			X
T.local_admin_LAN	X		X	X	X								(x)	(x)	X				(x)					X	X	(x)
T.remote_admin_WAN	X		X	X	X								(x)	(x)	X									X	X	(x)
T.counterfeit		X														X			X							(x)
T.Zert_Prüf				(x)		(x)		X					(x)	X	(x)	(x)										(x)
T.TimeSync				(x)		X							(x)	(x)	(x)	(x)	X									(x)
A.phys_Schutz																			X							
A.PF_LAN																				X						
A.SM-K																X										
A.sichere_TI																					X					
A.kein_DoS																						X				
A.AK																		X								
A.Betrieb_AK																							X			
A.Admin_EVG																								X		
A.Ersatzverfahren																										X

Tabelle 5: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen

Ein Kreuz „X“ in einer Zelle bedeutet, dass die in der Zeile des Kreuzes stehende Bedrohung durch das in der Spalte des Kreuzes stehende Sicherheitsziel (für den EVG oder für die Umgebung) abgewehrt wird bzw. dass die in der Zeile des Kreuzes stehende Annahme auf das entsprechende Umgebungsziel abgebildet wird. Man beachte, dass Common Criteria die

Abbildung von Annahmen auf EVG-Sicherheitsziele verbietet; der entsprechende Bereich der Tabelle ist daher grau schattiert.

Ein in Klammern gesetztes kleines Kreuz (x) bedeutet, dass das Ziel optional zur Abwehr der Bedrohung beitragen kann. Es steht dem ST-Autor frei, entsprechende Beziehungen zu ergänzen (ein kleines Kreuz (x) kann also sowohl gelöscht als auch durch ein großes Kreuz X ersetzt werden); siehe Application Note 130:.

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

- Die Abwehr von T.local_TOE_LAN wird durch die Klasse ADV und die Familie AVA_VLA unterstützt.
- Die Abwehr von T.counterfeit wird durch die Komponenten ADO_DEL.2 und ADO_IGS.1 unterstützt.
- Das Ziel **OE.Admin_EVG** wird durch die Familien AGD_ADM und AVA_MSU unterstützt.

Application Note 130: Abhängig von der Ausgestaltung des Netzkonnektors kann sich die **Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen** gegenüber diesem Schutzprofil noch leicht verändern. Der ST-Autor soll die tatsächlichen Produkteigenschaften beschreiben und abhängig davon die Inhalte in Tabelle 5 und im Folgenden Erklärungstext (Abschnitte 6.1.1 und 6.1.2) entsprechend anpassen.

Werden im Rahmen solcher Anpassungen Beziehungen ergänzt (d.h.: in Tabelle 5 werden Kreuzchen ergänzt), so ist dies kurz zu erläutern. Im Allgemeinen sollten aber keine Beziehungen (bzw. Kreuzchen) gestrichen werden (Ausnahme: Das Löschen kleiner Kreuzchen (x) in Klammern ist zulässig); falls ein großes Kreuzchen X gelöscht werden soll, so ist dies ausführlich zu begründen und mit der Prüfstelle abzustimmen. Insbesondere ist darauf zu achten, dass alle Bedrohungen weiterhin vollständig und effektiv abgewehrt werden und keine leeren Zeilen oder Spalten entstehen, in denen sich nicht wenigstens ein großes Kreuzchen X befindet.

6.1.2. Abwehr der Bedrohungen durch die Sicherheitsziele

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 5 auf die Bedrohungen abgebildeten Sicherheitsziele geeignet sind, um die Bedrohungen abzuwehren.

6.1.2.1. T.local_TOE_LAN

T.local_TOE_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.PF_LAN**; mit grundlegender Intrusion Prevention-Funktionalität); dieser schützt den EVG vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer. Im Fall einer Einbox-Lösung schützt der EVG (O.PF_LAN) auch den Anwendungskonnektor vor LAN-seitigen Angriffen; wenn im Fall einer Mehrkomponenten-lösung der EVG diesen Schutz nicht leisten kann, schützt ein dynamischer Paketfilter in der IT-Umgebung (vgl. **OE.PF_LAN**) den Anwendungskonnektor und trägt somit zur Abwehr

der Bedrohung bei. Der dynamische Paketfilter wird dabei unterstützt von **O.Protokoll**, indem sicherheitsrelevante Ereignisse protokolliert werden (z.B. die letzte vorgenommene Konfigurationsänderung oder auch der Zeitpunkt und die Versionsnummer eines gegebenenfalls eingespielten Software-Updates), und von **O.Schutz**, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse sicher gespeichert und nach Benutzung aktiv gelöscht werden.

Optional kann auch **O.Stateful** bei der Abwehr von T.local_TOE_LAN unterstützen, indem sicherheitsrelevante Ereignisse protokolliert werden. Siehe auch Application Note 130:.

6.1.2.2. T.remote_TOE_WAN

T.remote_TOE_WAN beschreibt einen Angriff aus dem Transportnetz, bei dem der Netzkonnektor bzw. dessen Integrität bedroht wird. Angriffe aus dem Transportnetz werden durch den VPN-Tunnel und den dynamischen Paketfilter (mit grundlegender Intrusion Prevention-Funktionalität) abgewehrt: Anfragen, die ein Angreifer durch den VPN-Tunnel zu senden versucht, werden vom Netzkonnektor als ungültig erkannt (weil der Angreifer die VPN-Schlüssel nicht kennt, **O.VPN_Integrität**) und verworfen. Das SM-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (**OE.SM-K**). Die Inhalte, die durch den VPN-Tunnel übertragen werden, sind nicht bösartig (**OE.sichere_TI**). Anfragen außerhalb des VPN-Tunnels werden durch den dynamischen Paketfilter gefiltert (**O.PF_WAN**) – der Netzkonnektor schützt sich selbst mittels des WAN-seitigen Paketfilters. Der WAN-seitige Paketfilter bietet zustandsgesteuerte Filterung (stateful packet inspection, zustandsgesteuerte Filterung, **O.Stateful**). Der dynamische Paketfilter wird dabei unterstützt von **O.Protokoll**, indem sicherheitsrelevante Ereignisse protokolliert werden (z.B. die letzte vorgenommene Konfigurationsänderung oder auch der Zeitpunkt und die Versionsnummer eines gegebenenfalls eingespielten Software-Updates), und von **O.Schutz**, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse sicher gespeichert und nach Benutzung aktiv gelöscht werden. Mit den gleichen Argumenten wie bei T.remote_VPN_Data (der Aufbau des sicheren Kanals wird vorab durch eine gegenseitige Authentisierung geschützt, die wiederum eine Zertifikatsprüfung und eine Überprüfung der Systemzeit umfasst), tragen auch die Ziele **O.VPN_Auth**, **O.Zert_Prüf**, **OE.PKI**, **O.Zeit**, **OE.Zeitsynchro** und **OE.RNG** zur Abwehr der Bedrohung bei.

6.1.2.3. T.remote_TOE_LAN

Angriffe aus dem Transportnetz werden durch den VPN-Tunnel und den dynamischen Paketfilter (mit grundlegender Intrusion Prevention-Funktionalität) abgewehrt: Anfragen, die ein Angreifer durch den VPN-Tunnel zu senden versucht, werden vom Netzkonnektor als ungültig erkannt (weil der Angreifer die VPN-Schlüssel nicht kennt, **O.VPN_Integrität**) und verworfen. Das SM-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (**OE.SM-K**). Die Inhalte, die durch den VPN-Tunnel übertragen werden, sind nicht bösartig (**OE.sichere_TI**). Anfragen außerhalb des VPN-Tunnels werden durch den dynamischen Paketfilter gefiltert (**O.PF_WAN**); der Netzkonnektor schützt durch diesen WAN-seitigen Paketfilter sich selbst und weitere dezentrale Komponenten im Praxis-LAN. Der dynamische Paketfilter wird dabei unterstützt von **O.Protokoll**, indem sicherheitsrelevante Ereignisse protokolliert werden. Konnte ein Primärsystem bereits kompromittiert werden, so unterstützt

auch der LAN-seitige Paketfilter beim Schutz des Netzkonnektors (**O.PF_LAN**): Im Fall einer Einbox-Lösung schützt der EVG (O.PF_LAN) auch den Anwendungskonnektor vor LAN-seitigen Angriffen. Wenn im Fall einer Mehrkomponentenlösung der EVG diesen Schutz nicht leisten kann, schützt ein dynamischer Paketfilter in der IT-Umgebung (vgl. **OE.PF_LAN**) den Anwendungskonnektor und trägt somit zur Abwehr der Bedrohung bei. Der EVG wird – wie bei T.remote_TOE_WAN – unterstützt von **O.Schutz**, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse sicher gespeichert und nach Benutzung aktiv gelöscht werden. Mit den gleichen Argumenten wie bei T.remote_VPN_Data (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.VPN_Auth**, **O.Zert_Prüf**, **OE.PKI**, **O.Zeit**, **OE.Zeitsynchro** und **OE.RNG** zur Abwehr der Bedrohung bei.

Optional kann auch **O.Stateful** bei der Abwehr von T.remote_TOE_LAN unterstützen, indem sicherheitsrelevante Ereignisse nicht nur – wie bei T.remote_TOE_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 Intrusion Prevention). Siehe auch Application Note 130:.

6.1.2.4. T.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.VPN_Vertraul**). Das SM-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (**OE.SM-K**). Dass die VPN-Schlüssel auf Seiten des VPN-Konzentrators geheim gehalten werden, dafür sorgt **OE.sichere_TI**. Dass die richtigen Daten auch tatsächlich verschlüsselt werden, dafür sorgt **OE.AK**, indem *zu schützende Daten* vom Anwendungskonnektor für den Netzkonnektor erkennbar gemacht werden, unterstützt von **OE.Betrieb_AK** (sicherer Betrieb des Anwendungskonnektors und der Primärsysteme). Der VPN-Client unterstützt die Entschlüsselung von Daten, die ihm der VPN-Konzentrator verschlüsselt zugesendet hat. Die Nutzdaten werden beim Senden integritätsgeschützt übertragen und beim Empfang auf ihre Integrität hin überprüft (**O.VPN_Integrität**), was Manipulationen ausschließt. Außerdem authentisieren sich die VPN-Partner gegenseitig zu Beginn der Kommunikation (**O.VPN_Auth**). Im Rahmen der gegenseitigen Authentisierung wird eine Zertifikatsprüfung durchgeführt (**O.Zert_Prüf**), die wiederum eine entsprechende PKI in der Umgebung voraussetzt (**OE.PKI**). Im Rahmen der Gültigkeitsprüfung von Zertifikaten benötigt der EVG eine sichere Zeitquelle (**O.Zeit** und regelmäßige Synchronisation mit einem Dienst in der Umgebung, **OE.Zeitsynchro**). Die Schlüssel für die VPN-Authentisierung liegen im sicheren Schlüsselspeicher. Die SM-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (**OE.RNG**), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Sichere Ersatzverfahren (**OE.Ersatzverfahren**) unterstützen bei der Abwehr aller Angriffe, die sich gegen Schwächen in kryptographischen Algorithmen und Protokollen richten.

Application Note 131: Optional kann auch O.Protokoll (Security Log) bei der Abwehr von T.remote_VPN_Data unterstützen, indem auch sicherheitsrelevante Ereignisse im Zusammenhang mit dem VPN-Client protokolliert werden (Schreiben von Audit-Daten zur späteren Auswertung oder forensischen Analyse nach einem Angriff). Siehe auch Application Note 130:.

6.1.2.5. T.local_admin_LAN

T.local_admin_LAN betrachtet Angriffe im Zusammenhang mit lokaler Administration des EVG. Der EVG muss dazu eine Zugriffskontrolle implementieren, so dass Administration nur durch Administratoren nach erfolgreicher Authentisierung möglich (**O.Admin_EVG**) ist. Die Administratoren halten dazu ihre Authentisierungsinformationen geheim (**OE.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 (unbefugtes Software-Update bzw. Aufbringen schadhafter Software, Zugriff auf Schlüssel) werden durch weitere Ziele verhindert: Die Software-Aktualisierung wird durch ein sicheres Protokoll vorgenommen (**O.Update**) und die übertragenen Updates sind frei von Schadfunktionen (**OE.Update**). Die vom EVG für die Integritätsprüfung verwendeten Schlüssel werden im sicheren Schlüsselspeicher verwahrt. Der Zugriff auf kryptographische Schlüssel und andere Geheimnisse im Arbeitsspeicher des EVGs wird durch sichere Speicherung und entsprechende Speicheraufbereitung verhindert (aktives Löschen nach Verwendung der Geheimnisse, **O.Schutz**). Administrative Tätigkeiten können im Ereignisprotokoll nachvollzogen werden (**O.Protokoll**). Die SM-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (**OE.RNG**), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Optional wirkt auch **O.Stateful** gegen diese Bedrohung, siehe die folgende Application Note 132:.

Application Note 132: Optional kann auch die Protokollierung gemäß O.Stateful zur Abwehr von T.local_admin_LAN und T.remote_admin_WAN beitragen, siehe Application Note 57:. Ebenfalls optional kann eine PKI in der IT-Einsatzumgebung (OE.PKI) genutzt werden, um den sicheren Kanal für die Administration aufzubauen. Falls im Rahmen der Administration kryptographische Verfahren zum Einsatz kommen (z.B. im Rahmen der Benutzerauthentisierung oder bei der Implementierung eines sicheren Kanals), trägt auch OE.Ersatzverfahren zur Abwehr von T.local_admin_LAN bei. Siehe auch Application Note 130: (Anpassung des Security Targets bei Bedarf).

6.1.2.6. T.remote_admin_WAN

T.remote_admin_WAN betrachtet Angriffe im Zusammenhang mit zentraler Administration. Hier gilt sinngemäß das gleiche wie unter T.local_admin_LAN und Application Note 132: Zur Abwehr tragen die Ziele **O.Admin_EVG**, **OE.Admin_EVG**, **O.Update**, **OE.Update**, **OE.RNG**, **O.Protokoll** und **O.Schutz** bei sowie optional auch **OE.PKI** und **OE.Ersatzverfahren**. Optional wirkt auch O.Stateful gegen diese Bedrohung, siehe auch oben, Application Note 132:.

6.1.2.7. T.counterfeit

Bei der Bedrohung T.counterfeit bringt ein Angreifer unbemerkt gefälschte Konnektoren in Umlauf. Neben der durch die Vertrauenswürdigkeitskomponente **ADO_DEL.2** geforderten Überprüfung des Auslieferungsverfahrens und entsprechenden Verfahren zur Inbetriebnahme (**ADO_IGS.1)** ermöglicht der EVG auf Anforderung einen Nachweis seiner Authentizität (**O.TOE_Authenticity**), der durch die kryptographische Identität im Sicherheitsmodul SM-K unterstützt wird (**OE.SM-K**). Der EVG wird an einem zutrittsgeschützten Ort aufbewahrt (**OE.phys_Schutz**), wodurch ein Entwenden erschwert wird. Sichere Ersatzverfahren (**OE.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.

6.1.2.8. T.Zert_Prüf

Bei der Bedrohung T.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.Zert_Prüf** abgewehrt. **OE.PKI** unterstützt, indem die Gegenseite die Anfragen signiert zurücksendet.

Application Note 133: Optional kann es im Rahmen der Gültigkeitsprüfung von Zertifikaten Plausibilitätsprüfungen geben, welche die Echtzeit des EVG verwenden; somit kann auch **O.Zeit** zur Abwehr von T.Zert_Prüf beitragen. Abhängig vom Umfang der Protokollierung können auch **O.Protokoll** und **O.Stateful** optional zur Abwehr von T.Zert_Prüf beitragen, siehe Application Note 57:. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der SM-K gespeichert sind, daher kann **OE.SM-K** optional bei der Abwehr von T.Zert_Prüf unterstützen. Ein externer Zufallszahlengenerator (**OE.RNG**) wird darüber hinaus als Lieferant für gute Zufallszahlen genutzt, die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Sofern bei T.Zert_Prüf kryptographische Verfahren zum Einsatz kommen, kann **OE.Ersatzverfahren** zur Abwehr beitragen. Das Security Target ist entsprechend anzupassen, siehe Application Note 132:.

6.1.2.9. T.TimeSync

T.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 **O.Zeit** abgewehrt, da das Ziel die Synchronisation über einen sicheren Kanal fordert. Die Zeit selbst wird durch die Umgebung (**OE.Zeitsynchro**) bereitgestellt, ebenso wie die Gegenseite des sicheren Kanals.

Application Note 134: Auch bei T.TimeSync können **O.Stateful** und **O.Protokoll** zur Abwehr der Bedrohungen beitragen; siehe Application Note 57:. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der SM-K gespeichert sind (**OE.SM-K** kann optional bei der Abwehr von T.TimeSync unterstützen). Ein externer Zufallszahlengenerator (**OE.RNG**) wird darüber hinaus als Lieferant für gute Zufallszahlen genutzt, die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Ebenfalls optional kann eine PKI in der IT-Einsatzumgebung genutzt werden, um einen sicheren Kanal für die Zeitsynchronisation aufzubauen (Beitrag von **OE.PKI** zur Abwehr von T.TimeSync). Sofern bei T.TimeSync kryptographische Verfahren zum Einsatz kommen, kann **OE.Ersatzverfahren** zur Abwehr beitragen. Das Security Target ist entsprechend anzupassen, siehe Application Note 132:.

6.1.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

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

6.2. Erklärung der Sicherheitsanforderungen

6.2.1. Überblick: Abbildung der Ziele auf Anforderungen

Die folgende Tabelle 6 orientiert sich zunächst an den in Abschnitt 2.4 definierten Sicherheitsdiensten des EVG. Sie ordnet jedem Sicherheitsdienst das zugehörige EVG-Sicherheitsziel zu und bildet dieses dann auf die zugehörigen (meist funktionalen) Anforderungen ab. Abhängigen Komponenten wurde ein Pfeil → vorangestellt. Der Schwerpunkt liegt bei dieser Darstellung auf den Sicherheitsdiensten (und damit auch Sicherheitszielen) für den EVG. Sicherheitsziele für die IT-Einsatzumgebung werden nicht berücksichtigt.

Anschließend werden in Abschnitt 6.2.1.1, Tabelle 7 die Sicherheitsziele des EVG und in Abschnitt 6.2.1.2, Tabelle 8 die Sicherheitsziele der Umgebung jeweils noch einmal direkt auf die zugehörigen Sicherheitsanforderungen abgebildet. Diese beiden Tabellen geben die durch Common Criteria[82] geforderten Inhalte wieder.

Sicherheitsdienst (s. Abschnitt 2.4)			**Sicherheitsziel**	**TSFR oder TSAR**
Nr.		**Dienst**		
1		VPN-Client		
	a)	gegenseitige Authentisierung der Endpunkte	O.VPN_Auth	FTP_ITC.1/VPN, FCS_COP.1/Sign, FCS_COP.1/Auth → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP
	b)	Vertraulichkeit und Datenintegrität der Nutzdaten (Verschlüsselung und Signatur) Status der VPN-Verbindung (Anzeige und Management)	O.VPN_Vertraul, O.VPN_Integrität	FTP_ITC.1/VPN, FCS_COP.1/Encrypt und FCS_COP.1/Hash → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP FMT_MOF.1
	c)	regelbasierte Informationsfluss-kontrolle (erzwungene VPN-Nutzung)	O.PF_WAN, O.PF_LAN	FDP_IFC.1/PF (Paketfilter) FDP_IFF.1/PF (Paketfilter) AVA_VLA.4 (hohes Angriffspotential)

[82] vgl. work units APE_REQ.1-18 und APE_REQ.1-19 bzw. ASE_REQ.1-18 und ASE_REQ.1-19

Sicherheitsdienst (s. Abschnitt 2.4)			Sicherheitsziel	TSFR oder TSAR
2		dynamischer Paketfilter mit zustandsgesteuerter Filterung (Intrusion Prevention)		
	a)	Paketfilter schützt den Konnektor und das LAN vor Angriffen a1) aus dem WAN und a2) aus dem LAN	O.PF_WAN, O.PF_LAN	FDP_IFC.1/PF (Paketfilter) → FDP_IFF.1/PF → FMT_MSA.3/PF (Default-Werte für die Paketfilter-Regeln) → FMT_MSA.1/PF (nur der Administrator darf die Filterregeln ändern) → FMT_SMR.1 (Rolle: Administrator) → FMT_SMF.1 (Ändern der Filterregeln ist eine administrative Funktion) AVA_VLA.4 (hohes Angriffspotential)
	b)	Separationsmechanismen für Mehrwertdienste (und ggf. Anwendungskonnektor) schützen TSF, TSF data und user data vor den Mehrwertdiensten; WAN-Verbindungen sind nach dem Aufbau der VPN Verbindung nur vom und zum VPN-Konzentrator möglich	O.Schutz	FPT_SEP.1/VAS
	c)	grundlegende Intrusion Prevention, dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	O.Stateful	FAU_SAA.1 → FAU_GEN.1/Stateful
3		Netzdienste		
	a)	Echtzeituhr mit Zeitsynchronisation, optional über einen sicheren Kanal (die maximal zulässige Abweichung schränkt den Missbrauch dieser Funktionalität durch einen Angreifer auch ohne	O.Zeit	FPT_STM.1/TOE (Echtzeituhr, eigene verlässliche Systemzeit) FPT_TDC.1/Time (regelmäßiger Abgleich via Netz; interpretation rules = max.

Sicherheitsdienst (s. Abschnitt 2.4)			Sicherheitsziel	TSFR oder TSAR
		sicheren Kanal hinreichend ein)		Zeitabweichung)
	b)	Gültigkeitsprüfung von Zertifikaten mit Sperrlisten	O.Zert_Prüf	FPT_TDC.1/Zert
4		Audit: Generierung von Audit-Daten zur späteren Auswertung mit dem Ziel der Intrusion Prevention	O.Stateful	FAU_GEN.1/Stateful
5		Selbstschutz		
	a)	Speicheraufbereitung (Schlüssel, z.B. VPN session keys, medizinische Daten); Ausnahmen: offline-Betrieb und Protokolldaten	O.Schutz	FDP_RIP.1
	b)	Selbsttests: teste eigene Integrität; Verwendung eines externen Vertrauensankers (SM-K) optional: physische Sicherheit	O.Schutz O.TOE_Authenticity	FPT_TST.1, FPT_AMT.1, FCS_COP.1/Hash, → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP FCS_COP.1/KeyExch, → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP ADO_DEL.2 ADO_IGS.1
	c)	sicherer Schlüsselspeicher für c1) kryptographische Identität als Netzkonnektor, c2) Prüfschlüssel für eigene Integrität (siehe 5 b)); optional: phys. Sicherheit	O.Schutz (für eigene Schlüssel und als Dienst für andere)	FDP_ACC.1/KeySt → FDP_ACF.1/KeySt → FMT_MSA.3/KeySt (Default-Werte für die Zugriffsrechte) → FMT_MSA.1/KeySt (Administration der Zugriffsrechte) FMT_MSA.2
	d)	Schutz von Geheimnissen, Side Channel-Resistenz	O.Schutz (Schutz gegen unbefugte Kenntnisnahme)	FPT_EMSEC.1
	e)	optional: sichere Kanäle zu anderen dezentralen Komponenten (Mehrkompo-		siehe Application Note 98:

Sicherheitsdienst (s. Abschnitt 2.4)			Sicherheitsziel	TSFR oder TSAR
		nentenlösung) sowie zum Anwendungskonnektor oder zur SMC-B		
	f)	Ereignisprotokoll (si-rel. Ereignisse mit Datum+Zeit)	O.Protokoll	FAU_GEN.1/Audit, FAU_GEN.2, FAU_STG.1, FAU_STG.3
6		Administration		
	a)	sicheres Update der Firmware und Software des Konnektors (Download, Prüfung der Integrität und Authentizität von Updates, optional Entschlüsselung, erst dann Aktivierung → Sequenz-kontrolle)	O.Update	FPT_ITI.1/Update FPT_RCV.4/Update FCS_COP.1/Sign → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP
	b)	Wartung: gesicherte Administration, evtl. sicherer Kanal (im LAN), Rolle Administrator	O.Admin_EVG	FTP_TRP.1/Admin (sicherer Kanal f. Wartung) FMT_SMR.1 (Rolle: Admin.)
	c)	erzwungene Authentisierung der Administratoren, Zugriffskontrolle für administrative Funktionen	O.Admin_EVG	FMT_MTD.1 (restrict management) → FMT_SMR.1 (Rolle: Admin.) → FMT_SMF.1 (Liste der Management-Funktionen) → FIA_UID.1/SMR → FIA_UAU.1/SMR

Tabelle 6: Abbildung der Sicherheitsdienste auf Ziele und Anforderungen

6.2.1.1. Abbildung der EVG-Ziele auf Anforderungen

EVG-Ziel	Aspekt des Ziels	SFR (TSFR, TSAR; vgl. Abschnitt 5.1.1 oder 5.1.2)
O.Schutz	Speicheraufbereitung: temporäre Kopien nicht mehr benötigter Geheimnisse werden unmittelbar nach Gebrauch aktiv überschrieben	FDP_RIP.1
	Selbsttests, Schutz gegen sicherheitstechnische Veränderungen	FPT_TST.1, FPT_AMT.1, FCS_COP.1/Hash, → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP
	sicherer Schlüsselspeicher: Schutz gespeicherter Geheimnisse gegen Auslesen und unbefugte Kenntnisnahme	FDP_ACC.1/KeySt, FDP_ACF.1/KeySt, FMT_MSA.3/KeySt, FMT_MSA.1/KeySt
	Schutz gegen unbefugte Kenntnis-nahme (Side Channel-Analysen)	FPT_EMSEC.1
	Separationsmechanismen für Mehrwertdienste (und ggf. Anwendungskonnektor)	FPT_SEP.1/VAS
O.Stateful	grundleg. Intrusion Prevention (2 c)): dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	FAU_GEN.1/Stateful, FAU_SAA.1
O.TOE_Authenticity	Auslieferungsverfahren: Nur authentische Netzkonnektoren können in Umlauf gebracht werden	FCS_COP.1/KeyExch, FCS_CKM.4, FMT_MSA.2, FDP_ITC.1/COP ADO_DEL.2 ADO_IGS.1
O.Admin_EVG	rollenbasierte Zugriffskontrolle für administrative Funktionen Identifikation und Authentisierung des Administrators Falls Administration nicht über dedizierten lokalen Anschluss (PS3) erfolgt, dann: sicherer Pfad	FMT_MTD.1, FMT_SMR.1, FIA_UID.1/SMR, FIA_UAU.1/SMR FTP_TRP.1/Admin (und Application Note 107:)

EVG-Ziel	Aspekt des Ziels	SFR (TSFR, TSAR; vgl. Abschnitt 5.1.1 oder 5.1.2)
	Aktivieren und Deaktivieren der Protokollierung = admin. Funktionen	FMT_SMF.1
O.Protokoll	EVG protokolliert si-rel. Ereignisse mit Daten und Zeitstempel (siehe O.Zeit)	FAU_GEN.1/Audit, FAU_GEN.2, FAU_STG.1, FAU_STG.3
O.Update	Prüfung der Integrität und Authentizität von Updates Aktivierung nur nach erfolgreichem Update (Sequenzkontrolle)	FPT_ITI.1/Update, FCS_COP.1/Sign, FCS_CKM.4, FMT_MSA.2, FDP_ITC.1/COP FPT_RCV.4/Update
O.Zeit	eigene verlässliche Systemzeit regelmäßiger Abgleich via Netz	FPT_STM.1/TOE FPT_TDC.1/Time
O.VPN_Auth	gegenseitige Authentisierung mit VPN-Konzentrator	FTP_ITC.1/VPN, FCS_COP.1/Auth FCS_COP.1/Sign, FCS_CKM.4, FMT_MSA.2, FDP_ITC.1/COP
O.Zert_Prüf	Gültigkeitsprüfung von Zertifikaten mit Hilfe von Sperrlisten	FPT_TDC.1/Zert
O.VPN_Vertraul	Vertraulichkeit der Nutzdaten im VPN	FTP_ITC.1/VPN, FCS_COP.1/Encrypt, → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP FMT_MOF.1
O.VPN_Integrität	Integrität der Nutzdaten im VPN	FTP_ITC.1/VPN FCS_COP.1/Hash, → FCS_CKM.4, → FMT_MSA.2, → FDP_ITC.1/COP FMT_MOF.1
O.PF_WAN	dynamischer Paketfilter zum WAN	FDP_IFC.1/PF, FDP_IFF.1/PF, FMT_MSA.3/PF, FMT_MSA.1/PF, FMT_SMR.1

EVG-Ziel	Aspekt des Ziels	SFR (TSFR, TSAR; vgl. Abschnitt 5.1.1 oder 5.1.2)
		FMT_SMF.1 AVA_VLA.4 (hohes Angriffspotential)
O.PF_LAN	dynamischer Paketfilter zum LAN,	FDP_IFC.1/PF, FDP_IFF.1/PF, FMT_MSA.3/PF, FMT_MSA.1/PF, FMT_SMR.1 FMT_SMF.1 AVA_VLA.4 (hohes Angriffspotential)
	regelbasierte Informationsflusskontrolle	FDP_IFF.1/PF (siehe Application Note 74:)

Tabelle 7: Abbildung der EVG-Ziele auf Anforderungen

6.2.1.2. Abbildung der Umgebungsziele auf Anforderungen

Umgebungsziel	Aspekt des Ziels, (IT-Ziel oder non-IT-Ziel)	SFR oder SAR, IT oder non-IT; Erläuterungen
OE.RNG	Externer Zufallszahlen-generator hoher Güte (IT-Ziel)	FCS_RND.1/Env, siehe Abschnitt 5.2.1
OE.Zeitsynchro	Bereitstellen eines Zeitstempels (IT-Ziel)	FPT_STM.1/Env, siehe Abschnitt 5.2.2
OE.PF_LAN	LAN-seitiger Paketfilter schützt AK vor potentiellen Angriffen aus dem LAN (IT-Ziel)	FDP_IFC.1/Env, siehe Abschnitt 5.2.4
OE.SM-K	sicherer Schlüsselspeicher für VPN-Schlüssel bzw. für Konnektoridentität (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.AK	Datenkennzeichnung durch Anwendungskonnektor und Primärsysteme (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.Admin_EVG	sichere Administration des EVG	

Umgebungsziel	Aspekt des Ziels, (IT-Ziel oder non-IT-Ziel)	SFR oder SAR, IT oder non-IT; Erläuterungen
	teilweise IT-Ziel, (Auswertung des Ereignisprotokolls) teilweise non-IT-Ziel (sichere Administration)	FAU_SAR.1/Env (Auswertung des Ereignisprotokolls), siehe Abschnitt 5.2.3 keine Auswahl aus CC Teil 2
OE.PKI	Betrieb einer PKI (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.phys_Schutz	Physischer Schutz des Netzkonnektors (non-IT-Ziel) (optional: IT-Ziel[83])	keine Auswahl aus CC Teil 2 (optional: Unterbringung in einem Gehäuse z.B. mit FPT_PHP.1/Env)
OE.sichere_TI	sichere Telematikinfrastruktur (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.kein_DoS	Gegenmaßnahmen gegen denial-of-service-Angriffe (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.Betrieb_AK	sicherer Betrieb des Anwendungskonnektors (non-IT-Ziel)	keine Auswahl aus CC Teil 2
OE.Update	Prozesse für sicheres Software-Update (non-IT-Ziel)	keine Auswahl aus CC Teil 2 Der vom EVG verwendete Prüfschlüssel wird bereits während der Produktion eingebracht. Der Hersteller muss dafür sorgen, dass ein Schlüssel geeigneter Länge und Qualität eingebracht wird
OE.Ersatzverfahren	sichere Ersatzverfahren bei Ausfall der Infrastruktur (non-IT-Ziel)	keine Auswahl aus CC Teil 2

Tabelle 8: Abbildung der Umgebungsziele auf Anforderungen

[83] Optional ist es möglich, den physischen Schutz als EVG-Ziel zu formulieren (in diesem Fall wäre ein zusätzliches EVG-Ziel O.Phys_Schutz zu formulieren).

6.2.1.3. Zusammenfassung: Abbildung der Ziele auf Anforderungen

	Sicherheitsziel für den EVG (O. ...) bzw. für die Umgebung (OE. ...)																									
Sicherheitsanforderung an den EVG **bzw. seine IT-Umgebung (.../Env)** **bzw. seine Non-IT-Umgebung (R. ...)**	O.Schutz	O.TOE_Authenticity	O.Admin_EVG	O.Protokoll	O.Update	O.Zeit	O.VPN_Auth	O.Zert_Prüf	O.VPN_Vertraul	O.VPN_Integrität	O.PF_WAN	O.PF_LAN	O.Stateful	OE.RNG	OE.Zeitsynchro	OE.PF_LAN	OE.SM-K	OE.AK	OE.Admin_EVG	OE.PKI	OE.phys_Schutz	OE.sichere_TI	OE.kein_DoS	OE.Betrieb_AK	OE.Update	OE.Ersatzverfahren
FTP_ITC.1/VPN							X		X	X																
FDP_IFC.1/PF											X	X														
FDP_IFF.1/PF											X	X														
FMT_MSA.3/PF											X	X														
FMT_MOF.1									X	X																
FPT_SEP.1/VAS	X																									
FPT_STM.1/TOE						X																				
FPT_TDC.1/Time						X																				
FPT_TDC.1/Zert								X																		
FAU_GEN.1/Stateful													X													
FAU_SAA.1													X													
FDP_RIP.1	X																									
FPT_TST.1	X																									
FPT_AMT.1	X																									
FDP_ACC.1/KeySt	X																									
FDP_ACF.1/KeySt	X																									
FMT_MSA.3/KeySt	X																									
FMT_MSA.1/KeySt	X																									
FPT_EMSEC.1	X																									
FAU_GEN.1/Audit				X																						
FAU_GEN.2				X																						
FAU_STG.1				X																						
FAU_STG.3				X																						
FMT_SMR.1			X								X	X														
FMT_MTD.1			X																							
FIA_UID.1/SMR			X																							
FIA_UAU.1/SMR			X																							
FTP_TRP.1/Admin			X																							
FMT_SMF.1			X								X	X														
FMT_MSA.1/PF											X	X														
FPT_ITI.1/Update					X																					
FPT_RCV.4/Update					X																					
FCS_COP.1/Hash	X									X																
FCS_COP.1/Auth							X																			

	Sicherheitsziel für den EVG (O. ...) bzw. für die Umgebung (OE. ...)																									
Sicherheitsanforderung an den EVG bzw. seine IT-Umgebung (.../Env) bzw. seine Non-IT-Umgebung (R. ...)	O.Schutz	O.TOE_Authenticity	O.Admin_EVG	O.Protokoll	O.Update	O.Zeit	O.VPN_Auth	O.Zert_Prüf	O.VPN_Vertraul	O.VPN_Integrität	O.PF_WAN	O.PF_LAN	O.Stateful	OE.RNG	OE.Zeitsynchro	OE.PF_LAN	OE.SM-K	OE.AK	OE.Admin_EVG	OE.PKI	OE.phys_Schutz	OE.sichere_TI	OE.kein_DoS	OE.Betrieb_AK	OE.Update	OE.Ersatzverfahren
FCS_COP.1/Encrypt									X																	
FCS_COP.1/KeyExch		X																								
FCS_COP.1/Sign					X		X																			
FCS_CKM.4	X	X			X		X		X	X																
FMT_MSA.2	X	X			X		X		X	X																
FDP_ITC.1/COP	X	X			X		X		X	X																
ADO_DEL.2		X																								
ADO_IGS.1		X																								
AVA_VLA.4											X	X														
FCS_RND.1/Env														X												
FPT_STM.1/Env															X											
FAU_SAR.1/Env																			X							
FDP_IFC.1/Env																X										

Tabelle 9: Abbildung der Ziele auf Anforderungen

6.2.2. Erfüllung der Sicherheitsziele durch die Anforderungen

In diesem Abschnitt wird erklärt, warum die Kombination der individuellen funktionalen Sicherheitsanforderungen (TSFR) und Anforderungen an die Vertrauenswürdigkeit (TSAR) für den EVG und für seine IT-Umgebung gemeinsam die formulierten Sicherheitsziele erfüllen. Dabei müssen die Anforderungen an den EVG die EVG-Ziele erfüllen und die Anforderungen an die IT-Umgebung die Ziele für die IT-Umgebung des EVG erfüllen.

6.2.2.1. Erfüllung der EVG-Sicherheitsziele

In Abschnitt 6.2.1 werden jedem Ziel bereits diejenigen Anforderungen zugeordnet, die gemeinsam das entsprechende Ziel abdecken. Tabelle 6 geht dabei nach Sicherheitsdiensten geordnet vor (vgl. Abschnitt 2.4), während Tabelle 7 direkt jedem Sicherheitsziel für den EVG die zugehörigen Sicherheitsanforderungen zuordnet.

Tabelle 7 ist wie folgt aufgebaut: Alle EVG-Sicherheitsziele aus Abschnitt 4.1 werden in der ersten Spalte („EVG-Ziel“) der Tabelle aufgelistet. Zu jedem Sicherheitsziel werden in der zweiten Spalte („Aspekt des Ziels“) die einzelnen Aspekte des Sicherheitsziels genannt: Jede geforderte Eigenschaft aus der Beschreibung eines EVG-Ziels findet sich in einem Aspekt wieder. Jedem solchen Aspekt werden in der dritten Spalte („SFR (TSFR, TSAR)“) die ihn umsetzenden Sicherheitsanforderungen zugeordnet. Aus dieser detaillierten Gegenüberstellung wird unmittelbar ersichtlich, dass die Kombination der entsprechenden Anforderungen den Aspekt des EVG-Sicherheitsziels vollständig abdeckt.

6.2.2.2. Erfüllung der Sicherheitsziele für die Umgebung

Tabelle 8 in Abschnitt 6.2.1 ist analog zur Tabelle 7 aufgebaut und ordnet den Sicherheitszielen für die Umgebung die zugehörigen Anforderungen zu. Für non-IT-Ziele ist keine Auswahl von Sicherheitsanforderungen aus dem Katalog CC Teil 2 [2] bzw. aus CC Teil 3 [3] erforderlich.

6.2.2.3. Gegenseitige Unterstützung und interne Konsistenz der Anforderungen

Aus Tabelle 6 ist ersichtlich, wie die Anforderungen den in Abschnitt 2.4 beschriebenen Sicherheitsdiensten zugeordnet wurden. Die Entwicklung der Anforderungen ausgehend von den Sicherheitsdiensten sorgt dafür, dass alle Aspekte berücksichtigt wurden und dass jeder Aspekt für sich genommen vollständig in Form von Anforderungen formuliert wurde.

In jeder Zeile in dieser Tabelle wurden neben der hauptsächlich das Ziel umsetzenden Anforderung auch einige der abhängigen Anforderungen aufgeführt. Die Erfüllung der durch CC Teil 2 [2] vorgegebenen Abhängigkeiten dient ebenfalls dazu die Vollständigkeit der Anforderungen und die interne Konsistenz sicherzustellen. Da durch die Abhängigkeiten häufig sehr umfangreiche Beziehungen aufgespannt werden, wurden nicht alle transitiven Abhängigkeiten aufgelistet, sondern die Kette der Abhängigkeiten wurde jeweils dort unterbrochen, wo eine abhängige Anforderung mehrheitlich einem anderen Sinnzusammenhang zugeordnet werden muss.

> Beispiel: Der von den Sicherheitszielen O.PF_WAN und O.PF_LAN geforderte dynamische Paketfilter (FDP_IFC.1/PF und FDP_IFF.1/PF) bedingt, dass die Paketfilter-

Regeln verwaltet werden (FMT_MSA.1/PF) und geeignete Voreinstellungen (Default-Werte, FMT_MSA.3/PF) für die Regeln existieren. Alle diese Anforderungen werden in den Zeilen zu O.PF_WAN und O.PF_LAN gelistet.

Die Anforderung FMT_MSA.1/PF wiederum impliziert, dass die Verwaltung nur von autorisierten Administratoren vorgenommen werden kann. Die Benutzeridentifikation und –authentisierung (FIA_UID.1/SMR, FIA_UAU.1/SMR) ist von ihrem Wesen her mehrheitlich dem Ziel O.Admin_EVG zuzuordnen. Daher wurden FIA_UID.1/SMR und FIA_UAU.1/SMR nicht in den Zeilen für die Sicherheitsziele O.PF_WAN und O.PF_LAN aufgelistet, sondern in den entsprechenden Tabellenzeilen zu O.Admin_EVG.

Die Gruppierung der Anforderungen nach Sicherheitsdiensten erlaubt es, zusammengehörige Anforderungen gemeinsam zu betrachten. Diese Vorgehensweise wird außerdem durch die Verwendung von Suffixen unterstützt („/PF“ für alle Anforderungen, die den Paketfilter betreffen; „/KeySt“ für alle Anforderungen, die den sicheren Schlüsselspeicher betreffen, „/Update“ für alle Anforderungen, die das sichere Software-Update betreffen). Gleichzeitig helfen die Suffixe, Iterationen derselben Komponente immer korrekt dem jeweiligen Kontext zuzuordnen (vgl. etwa FPT_TDC.1/Zert und FPT_TDC.1/Time). Anforderungen an die IT-Einsatzumgebung wurden mit dem Suffix „/Env“ gekennzeichnet.

6.2.3. Erfüllung der Abhängigkeiten

6.2.3.1. Erfüllung der funktionalen Anforderungen

In Abschnitt 5.1.1 wird für jede funktionale Anforderung die Menge aller von ihr abhängigen Komponenten unter dem Stichwort *Dependencies* aufgeführt. Die Erfüllung der Abhängigkeiten wird jeweils unter dem Stichwort *hier erfüllt durch:* demonstriert.

Wird eine Abhängigkeit nicht erfüllt, so wird unter dem Stichwort *Diese Abhängigkeit wird nicht erfüllt. Begründung:* diskutiert und begründet, weshalb die Abhängigkeit nicht erfüllt werden muss.

6.2.3.2. Erfüllung der Anforderungen an die Vertrauenswürdigkeit

Es wurde eine vollständige EAL-Stufe ausgewählt (EAL4) und anschließend augmentiert. Die EAL-Stufe an sich ist in sich konsistent und erfüllt alle Abhängigkeiten. Die Abhängigkeiten der im Rahmen der Augmentierung neu hinzugekommenen Komponenten ADV_IMP.2, AVA_MSU.3 und AVA_VLA.4 werden durch EAL4 ebenfalls erfüllt, wie die folgende Tabelle 10 zeigt.

Augmentierung	Abhängigkeit(en)	Bewertung	Erfüllung der Abhängigkeit?
ADV_IMP.2	ADV_LLD.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	ALC_TAT.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
AVA_MSU.3	ADO_IGS.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	ADV_FSP.1	ADV_FSP.2 ist Bestandteil von EAL4	Abhängigkeit ist erfüllt

Augmen-tierung	Abhängig-keit(en)	Bewertung	Erfüllung der Abhängigkeit?
	AGD_ADM.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	AGD_USR.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
AVA_VLA.4	ADV_FSP.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	ADV_HLD.2	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	ADV_IMP.1	ADV_IMP.1 ist Bestandteil von EAL4, ADV_IMP.2 wurde augmentiert	Abhängigkeit ist erfüllt
	ADV_LLD.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	AGD_ADM.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt
	AGD_USR.1	ist Bestandteil von EAL4	Abhängigkeit ist erfüllt

Tabelle 10: Erfüllung der Abhängigkeiten der augmentierten Komponenten

6.3. Erklärung für Erweiterungen und Definition erweiterter Familien

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_EMSEC.1. Diese erweiterte Komponente wurde bereits im SSCD-PP [14], Abschnitt 6.6.1, definiert und motiviert. Die wichtigsten Argumente der Begründung werden im Folgenden wiedergegeben.

Der EVG soll Angriffe verhindern, die sich gegen den privaten Authentisierungsschlüssel für das VPN (FTP_ITC.1/VPN) und andere vom EVG verarbeitete Geheimnisse richten, wobei die Angriffe extern beobachtbare physikalische Phänomene ausnutzen. Der EVG soll den Abfluss von geheimen Informationen wirkungsvoll verhindern. Ein Beispiel für solche Angriffe sind Timing-Angriffe; für weitere Details siehe die Diskussion in Abschnitt 7.6.17. Die Familie FPT_EMSEC beschreibt die funktionalen Anforderungen an eine Beschränkung der ausnutzbaren Ausstrahlung.

Die erweiterte Familie FPT_EMSEC wird im Folgenden Abschnitt 6.3.1 definiert.

Darüber hinaus war eine Erweiterung des CC Teil 2 [2] erforderlich, um die funktionale Anforderung FCS_RND.1/Env an den externen Zufallszahlengenerator in der IT-Einsatzumgebung zu formulieren (vgl. Abschnitt 5.2.1). Diese Erweiterung ist dadurch zu begründen, dass der Katalog in CC Teil 2 [2] keine Möglichkeiten vorsieht, eine solche Anforderung zu spezifizieren. Gleichzeitig wird die Familie FCS_RND seit vielen Jahren

erfolgreich in Evaluierungen verwendet, wie beispielsweise die häufige Verwendung des Smartcard IC Platform Protection Profiles [15] vom Juli 2001 belegt. Auch in das *Common Criteria Protection Profile Secure Module Card (PP-SMC)* [13] wurde FCS_RND bereits aufgenommen.

Die erweiterte Familie FCS_RND wird im unten folgenden Abschnitt 6.3.2 definiert.

6.3.1. Definition der erweiterten Familie FPT_EMSEC und der Anforderung FPT_EMSEC.1

Die Definition der Familie FPT_EMSEC wurde aus dem *Common Criteria Protection Profile – Secure Signature-Creation Device (SSCD)* Type 3 [14], Abschnitt 6.6.1, übernommen.

Family	**FPT_EMSEC – TOE Emanation**
Family behaviour	This family defines requirements to mitigate intelligible emanations.
Component levelling:	**FPT_EMSEC – TOE Emanation** — 1

FPT_EMSEC.1 – TOE Emanation has two constituents:

- FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
FPT_EMSEC.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_EMSEC.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*].
Dependencies:	No dependencies.

6.3.2. Definition der erweiterten Familie FCS_RND und der Anforderung FCS_RND.1

Die Definition der Familie FCS_RND wurde aus dem *Common Criteria Protection Profile Secure Module Card (PP-SMC)* [13], Abschnitt 5.1, übernommen.

Family	**FCS_RND – Generation of random numbers**
Family behaviour	This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.
Component levelling:	**FCS_RND – Generation of random numbers** — 1
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management :	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].
Dependencies:	No dependencies.

6.4. Erklärung für die gewählte EAL-Stufe

Der Netzkonnektor stellt die Verbindung zwischen den dezentralen Komponenten eines Leistungserbringers und der zentralen Telematikinfrastruktur 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* befinden, muss davon ausgegangen werden, dass aus dem Transportnetz Angriffe gegen den Netzkonnektor mit hohem Angriffspotential durchgeführt werden.

Damit die Evaluierung nachweisen kann, dass der Netzkonnektor diese Angriffe erfolgreich abwehrt, muss eine Schwachstellenanalyse durchgeführt werden, die genau dieses hohe

Angriffspotential berücksichtigt. Deshalb wurde AVA_VLA.4 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_VLA.4 definierten Abhängigkeiten wider (insbesondere ADV_HLD.2, ADV_LLD.1 und ADV_IMP.1; siehe auch Tabelle 10 in Abschnitt 6.2.3.2 oben). Zieht man diese Komponenten in Betracht, so ergibt sich, dass nur eine Evaluierung nach einer sehr stark augmentierten Stufe EAL3+ oder nach der Stufe EAL4+ überhaupt in Frage kommen. In diesem Fall wurde schließlich zugunsten der noch sichereren Stufe EAL4+ entschieden.

Siehe auch Sicherheitskonzept – Offline [27], Abschnitt 4.4.2.1.1; dort heißt es:

„Aufgrund seiner zentralen sicherheitstechnischen Position des Konnektors ist mindestens eine Sicherheitseinstufung nach dem

- *Common Criteria Evaluation Assurance Level 4 (EAL4) / ISO 15408*
- *inklusive der Prüfung gegen hohes Angriffspotenzial (AVA_VLA.4)*

auf Basis eines Protection Profiles notwendig.“

6.5. Erklärung für die gewählte Funktionsstärke (SOF: high)

Da der EVG Angreifern mit hohem Angriffspotential widerstehen können soll (AVA_VLA.4 ist Teil der gewählten Assurance-Anforderungen, vgl. Abschnitt 6.4), muss er auch direkten Angriffen mit hohem Angriffspotential widerstehen können. Somit ergibt sich sofort die Forderung nach hoher Funktionsstärke (AVA_SOF.1, Strength of function: high).

7. Anhang

7.1. Gesetzliche Anforderungen

Das fünfte Sozialgesetzbuch [5] fordert in § 291a „Elektronische Gesundheitskarte“ die Erweiterung der Krankenversichertenkarte zu einer elektronischen Gesundheitskarte und definiert darin die Pflichtanwendungen

- Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form (sogenanntes elektronisches Rezept oder „eRezept“) und
- Berechtigungsnachweis zur Inanspruchnahme von medizinischen Leistungen (dies umfasst – wie schon bisher durch die Krankenversichertenkarte – die Abfrage von Versichertenstammdaten und Zuzahlungsstatus).

Ferner definiert das Gesetz die folgenden freiwilligen Anwendungen, bei denen dem Versicherten die Teilnahme freigestellt wird:

- Speicherung von medizinischen Notfalldaten (beispielsweise zum Abruf dieser Daten durch den Notarzt an einem Unfallort),
- elektronischer Arztbrief (auf diese Weise sollen Ärzte im Falle einer Überweisung eines Versicherten Befunde, Diagnose, Therapieempfehlungen sowie Behandlungsberichte austauschen können),
- Speicherung von Daten zur Prüfung der Arzneimitteltherapiesicherheit (das Ziel ist hier die frühzeitige Erkennung von Arzneimittelunverträglichkeiten) und
- Speicherung von Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (sogenannte „elektronische Patientenakte“),
- Speicherung von durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten, sowie
- Speicherung von Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten.

Im Rahmen der genannten freiwilligen Anwendungen werden Daten erhoben, gespeichert, verarbeitet und genutzt.

Der Konnektor unterstützt sowohl Pflichtanwendungen als auch freiwillige Anwendungen. Anforderungen an den Konnektor wurden bisher nur aus den Pflichtanwendungen abgeleitet.

Application Note 135: Der Anwendungskonnektor ist dafür verantwortlich, dass medizinische Daten, die vom Netzkonnektor verarbeitet werden, bereits kryptographisch verschlüsselt sind, wenn sie an den Netzkonnektor übergeben werden.

7.2. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AH	Authentication Header, siehe RFC 2402 und RFC 4302 [35]
AK	Anwendungskonnektor, umfasst im weiteren Sinne die Informationsflusskontrolle und Anwendungslogik (IFK/AL) sowie die Signaturanwendungskomponente (SAK), umfasst im engeren Sinne nur die Informationsflusskontrolle und Anwendungslogik (IFK/AL)
AK i.e.S.	AK im engeren Sinne (IFK/AL)
AK i.w.S.	AK im weiteren Sinne (AK und SAK mit Trusted Viewer und Darstellungskomponente)
AK-PP	Schutzprofil (Protection Profile) für den Anwendungskonnektor (im engeren Sinne)
AL	Anwendungslogik, siehe auch AK und IFK/AL
AVS	Apothekenverwaltungssystem
BA	Berufsausweis
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (siehe www.bundesnetzagentur.de)
BNetzA-PP	Schutzprofil (Protection Profile, PP) der Bundesnetzagentur (BNetzA); in diesem Zusammenhang speziell das BNetzA-PP für Signaturanwendungskomponenten
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAMS	Card Application Management System
CRL, CRLs	Certificate Revocation List(s)
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information (siehe www.dimdi.de) , eine nachgeordnete Behörde des Bundesministeriums für Gesundheit (BMG)
DoS	denial of service, übersetzt etwa Dienstverweigerung; bezeichnet einen Angriff auf einen Server mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen; in der Regel geschieht dies durch Überlastung
DSL	Digital Subscriber Line
DTBS	data to be signed, zu signierende Daten (Begriff aus dem SSCD-PP [14])
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card (englischer Begriff für eGK)
ESP	Encapsulating Security Payload; siehe RFC 4303 [36]

Abkürzung	Bedeutung
EVG	Evaluierungsgegenstand
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, siehe www.gematik.de
GKV	gesetzliche Krankenversicherung
HBA	Heilberufsausweis
HPC	Health Professional Card (englischer Begriff für HBA)
HSM	High Security Modul, Hochsicherheitsmodul; sicherer Schlüsselspeicher mit der Möglichkeit, kryptographische Berechnungen auszuführen, ohne dass das Schlüsselmaterial das HSM verlässt
ICMP	Internet Control Message Protocol, siehe RFC 792
IFK	Informationsflusskontrolle
IFK/AL	Informationsflusskontrolle und Anwendungslogik, einer der Hauptfunktionsblöcke des Konnektors (siehe auch AK, NK und SAK)
IKE	Internet Key Exchange, siehe RFC 2409 [37] und RFC 4306 [38]
IP	Internet Protocol
IPsec	IP Security, vgl. RFC2401 bzw. RFC4301 [34]
IPv4	Internet Protocol version 4, siehe RFC 791 (www.ietf.org/rfc/rfc791.txt)
IPv6	Internet Protocol version 6, siehe RFC 2460 (www.ietf.org/rfc/rfc2460.txt)
KIS	Krankenhausinformationssystem
KV	Kassenärztliche Vereinigung
LAN	lokales Netzwerk (local area network), meist im Zusammenhang mit dem lokalen Netzwerk eines Leistungserbringers verwendet
LS*n*	logische Schnittstelle Nr. *n* (siehe Abschnitt 2.2.2)
MAC	Message Authentication Code; kryptographische Prüfsumme zum Schutz der Datenintegrität; vergleichbar einer Signatur, aber erstellt unter Verwendung eines symmetrischen Kryptoalgorithmus’
NAT	Network Address Translation, siehe RFC 2663
NK	Netzkonnektor, einer der Hauptfunktionsblöcke des Konnektors (siehe auch AK sowie SAK und IFK/AL)
NK-PP	Schutzprofil (Protection Profile) für den Netzkonnektor
NTP	Network Time Protocol, siehe RFC 958 (Sept. 1985) und NTP Version 4 Release Notes (Okt. 2005)
OCSP	Online Certificate Status Protocol, siehe RFC 2560
PIN	Persönliche Identifikationsnummer, dient zur Authentisierung eines menschlichen Benutzers gegenüber einem IT-System (hier: SM-K)

Abkürzung	Bedeutung
PKV	private Krankenversicherung
PP	Protection Profile (Schutzprofil)
PS	Primärsystem
PS*n*	physische Schnittstelle Nr. *n* (siehe Abschnitt 2.2.1)
PVS	Praxisverwaltungssystem
RFC	Request for comment, siehe http://tools.ietf.org/html/
RSA	asymmetrisches Kryptoverfahren, benannt nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman
SAK	Signaturanwendungskomponente (hier stets: Signaturanwendungskomponente des Konnektors), einer der Hauptfunktionsblöcke des Konnektors (siehe auch NK und IFK/AL)
SGB V	Sozialgesetzbuch, fünftes Buch; dessen § 291a beschreibt die Einführung der elektronischen Gesundheitskarte
SICCT	Secure Interoperable Chip Card Terminal, Kartenleser
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC	Secure Module Card, Sicherheitsmodul (hier: Chipkarte als sicherer Schlüsselspeicher, siehe auch *Common Criteria Protection Profile Secure Module Card (PP-SMC)* [13])
SMC-B	Secure Module Card, Typ B, Träger der kryptographischen Identität der Organisation des Leistungserbringers; wird u.a. vom Anwendungskonnektor (im engeren Sinne) zur Authentisierung gegenüber zentralen Diensten (Message Broker, Fachanwendungen) verwendet
SM-K	Sicherheitsmodul (für den) Netzkonnektor, Träger der kryptographischen Identität des Netzkonnektors; wird u.a. vom Netzkonnektor zur Authentisierung gegenüber der zentralen Telematikinfrastruktur verwendet (VPN-Konzentrator)
SNTP	Simple Network Time Protocol, siehe RFC 4330
SSCD	Secure Signature Creation Device, englisches Pendant zu SSEE
SSEE	Sichere Signaturerstellungseinheit, deutsches Pendant zu SSCD
SSL	Secure Sockets Layer, sicheres Kommunikationsprotokoll; siehe auch TLS
ST	Security Target
ST-Autor	Autor des Security Targets (welches basierend auf diesem PP erstellt wird)
TAE	Telekommunikationsanschlusseinheit
TCP	Transmission Control Protocol, siehe RFC 793 und RFC 1323

Abkürzung	Bedeutung
TOE	Target of evaluation, englisches Synonym für EVG
TLS	Transport Layer Security, TLS 1.0 und TLS 1.1 sind standardisierte Weiterentwicklungen des SSL-Protokolls (zuletzt SSL 3.0, siehe SSL).
TSAR	TOE Security Assurance Requirement, Anforderung an die Vertrauenswürdigkeit des EVG
TSFR	TOE Security Functional Requirement, funktionale Sicherheitsanforderung an den EVG
TV	Trusted Viewer, sichere Anzeigekomponente der SAK gemäß SigG/SigV
UDP	User Datagram Protocol, siehe RFC 768
USB	Universal Serial Bus
VAD	verification authentication data, vom Heilberufler (bzw. Versicherten) eingegebene PIN (im Gegensatz zur auf der Karte gespeicherten Referenz-PIN, gegen die die eingegebene PIN verglichen wird), welche die Signaturfunktion des HBA bzw. der eGK freischaltet (Begriff aus dem SSCD-PP [14])
VODD	Verordnungsdaten-Dienst; zentraler Dienst zur Verwaltung von Verordnungen (umgangssprachlich: „Rezepten“)
VPN	virtuelles (nur logisch getrennt existierendes) privates Netz (virtual private network) Ein VPN nutzt ein offenes, ungeschütztes Netz (z.B. das Internet) als Transportmedium und ermöglicht darauf eine gesicherte Verbindung zwischen den rechtmäßigen Teilnehmern des VPNs, die sich durch den Besitz kryptographischer Schlüssel als solche ausweisen. Die in einem VPN übertragenen Daten werden in aller Regel durch Verschlüsselung gegen unbefugte Kenntnisnahme und durch kryptographische Prüfsummen gegen unbemerkte Veränderung geschützt.
VPN-K	VPN-Konzentrator
VSD	Versicherten-Stammdaten
VSDD	Versicherten-Stammdaten-Dienst (zentraler Dienst)
WAN	Weitverkehrsnetzwerk (wide area network), meist im Zusammenhang mit dem Transportnetz zur Anbindung der Leistungserbringer an die entfernte Telematikinfrastruktur verwendet; beispielsweise kann das Internet als Transportmedium für ein VPN genutzt werden
X.509	Standard der ITU-T (International Telecommunication Union) für Public Key Infrastrukturen und insbesondere für den Aufbau von Zertifikaten

Tabelle 11: Abkürzungsverzeichnis

7.3. Glossar

Begriff	Bedeutung
application connector	Anwendungskonnektor
attacker	Angreifer (siehe auch Abschnitt 3.3.1 Subjekte)
care provider	Leistungserbringer
central telematics infrastructure	zentrale Telematikinfrastruktur
network connector	Netzkonnektor
Secure Viewer	Sichere Anzeigekomponente (als Teil einer Signaturanwendungs-komponente) im Sinne des § 17 (2) SigG [7], an anderem Ort manchmal auch als Trusted Viewer bezeichnet
stateful packet inspection, stateful inspection	dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird; der Verbindungsstatus eines Datenpakets wird in die Entscheidung einbezogen, ob ein Informationsfluss zulässig ist oder nicht
Trusted Viewer	Sichere Anzeigekomponente, Synonym zu Secure Viewer, siehe auch dort
value-added services	Mehrwertdienste
VPN concentrator	VPN-Konzentrator
workstation	Primärsystem bzw. Arbeitsplatz des Primärsystems

Tabelle 12: Glossar

7.4. Abbildungsverzeichnis

7.5. Tabellenverzeichnis

7.6. Anwendungshinweise (Application Notes) für den Autor des Security Targets

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

7.6.1. Sperrung kryptographischer Identitäten (zu Abschnitt 2, kryptographische Identität)

Technisch besteht grundsätzlich die Möglichkeit vor, einzelne (z.B. gestohlen gemeldete) EVGs oder auch ganze Baureihen von EVGs zu sperren (z.B. bei Bekanntwerden eines Problems, welches eine gesamte Baureihe betrifft), indem die entsprechenden Zertifikate gesperrt bzw. zurückgerufen werden. Solche Aspekte liegen außerhalb dieses Schutzprofils und müssen in einem Betriebskonzept adressiert werden.

7.6.2. Bösartige Software auf Primärsystemen (zu Abschnitt 2.1 und zu Abschnitt 3.6, A.AK)

In Abschnitt 2.1 Einsatzumgebung des Konnektors heißt es: „*Es muss davon ausgegangen werden, dass sich auf einem Primärsystem auch schadhafte (bösartige) Software befinden kann.*“ Dazu ist anzumerken:

Obwohl das Vorhandensein bösartiger Software auf Primärsystemen durch die Annahme A.Betrieb_AK verhindert werden soll, muss nach dem Stand der Technik davon ausgegangen werden, dass Leistungserbringer eine Kompromittierung eines ihrer Primärsysteme nicht sicher verhindern bzw. nicht in jedem Fall frühzeitig erkennen können. Dieses Schutzprofil betrachtet daher auch Angriffe aus dem LAN heraus gegen den Netzkonnektor (an seiner LAN-seitigen Schnittstelle), siehe dazu die Bedrohungen T.local_TOE_LAN und

T.remote_TOE_LAN in den Abschnitten 3.4.2.1 und 3.4.2.3 sowie die Ausführungen zu Leistungserbringern in Abschnitt 3.3.1.

7.6.3. Aufbau und physische Abgrenzung des Netzkonnektors (zu Abschnitt 2.3)

Zuordnung der Basisdienste zu Konnektorteilen: Bei einer Realisierung des Konnektors als Mehrbox-Lösung (siehe auch Application Note 6:) soll der ST-Autor beschreiben, welche einzelne Bestandteile des Konnektors ggf. mehrfach vorhanden sind und/oder welche Dienste durch mehrere Konnektorteile gemeinsam genutzt werden.

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

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

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

Reine Software-Lösungen: Realisierungen eines Konnektors als reine Software-Lösungen sind grundsätzlich denkbar, beispielsweise „begehbare Konnektoren“ in Form eines Serverraums in einem Krankenhaus. In jedem Fall muss die Umgebung des Konnektors für physische Sicherheit sorgen (sicherer Raum mit Zutrittskontrolle, siehe A.phys_Schutz). Die Nutzung eines Sicherheitsmoduls (SM-K, beispielsweise in einer Ausprägung als Chipkarte oder als Hochsicherheitsmodul (HSM)) zum Nachweis der Bauartzulassung ist auch in diesem Fall erforderlich. Siehe auch Application Note 4: Möglichkeit zur Differenzierung und Application Note 60:. Die Implementierung muss aber hinreichend resistent gegen Angriffe sein (AVA_VLA.4) und zum Nachladen von ausführbarem Code muss eine hinreichend strenge Separation vom EVG durchgesetzt werden (etwa gemäß FPT_SEP.2).

Im Falle einer aus Hardware und Software bestehenden Lösung kann der Konnektor sich physisch über mehrere Gehäuse verteilen (**Mehrkomponentenlösung** oder Mehrbox-Lösung) oder Anwendungskonnektor und Netzkonnektor können im selben Gehäuse vereint sein (Einbox-Lösung). Gleiches gilt sinngemäß für reine Software-Lösungen: Die Funktionalitäten von Anwendungskonnektor und Netzkonnektor können in einem Programm-Modul vereint oder über mehrere Module verteilt sein. Siehe dazu auch Application Note 6: Einbox- vs. Mehrbox-Lösung und Zuordnung der Basisdienste zu Konnektorteilen (weiter oben).

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

Sicherheitsfunktionalität des Betriebssystems zu nutzen, ohne dass diese evaluiert wird. Siehe dazu auch die Diskussion „*Betriebssystem als Bestandteil des EVGs*“ in Abschnitt 7.6.4.

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

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

- Sofern der zusätzliche Code zum Evaluierungszeitpunkt bereits bekannt ist, kann seine Unschädlichkeit im Rahmen der Evaluierung überprüft werden. Der Code kann dann nach der Zertifizierung nicht mehr verändert werden, ohne den zertifizierten Status des Netzkonnektors zu verlieren.
- Sofern der Code zum Evaluierungszeitpunkt noch nicht bekannt ist oder gar die Möglichkeit zur Aktualisierung solchen Codes gegeben sein soll, muss der EVG über entsprechende Separationsmechanismen verfügen. Im Security Target kann dies durch die Anforderung aus der Familie FPT_SEP oder eine äquivalente Anforderung an den EVG abgebildet werden. Durch die Separationsmechanismen muss sichergestellt werden, dass Störungen der evaluierten Funktionalität des Netzkonnektors ausgeschlossen sind und dass allen durch den Anwendungskonnektor oder durch die Einführung eventueller Mehrwertdienste entstehenden Bedrohungen wirksam begegnet wird.

Der Hersteller des EVGs soll eine klare Aussage in das Security Target aufnehmen, ob zusätzlicher ausführbarer Code auf dem Konnektor vorhanden bzw. zulässig ist und ob Separationsmechanismen im Rahmen der Evaluierung untersucht werden sollen. In diesem Fall sind ein geeignetes Sicherheitsziel für den EVG sowie entsprechende funktionale Anforderungen (z.B. FPT_SEP.2) zu ergänzen. Das Sicherheitsziel wiederum muss von einer Bedrohung (z.B.: Fehler in anderer Software-Komponente) oder einer organisatorischen Sicherheitspolitik (z.B.: es soll weitere Software auf der Plattform ablaufen können, auf der der Konnektor implementiert ist) abgeleitet werden.

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

- Die **Anzeige der Betriebsbereitschaft und des Bestehens einer VPN-Verbindung** zur zentralen Telematikinfrastruktur kann beispielsweise durch Leuchtdioden am Gehäuse eines aus Hardware und Software bestehenden (Netz-)Konnektors implementiert sein, aber auch in Form einer http-basierten Bedieneroberfläche, die an der LAN-Schnittstelle des Netzkonnektors bereitgestellt wird; die Darstellung könnte dann z.B. auf dem Browser eines im LAN installierten PCs erfolgen. Lösungen, die beides kombinieren, sind bereits seit einiger Zeit marktüblicher Standard z.B. bei DSL-Routern mit Paketfilter-Funktionalität für den Heimgebrauch.
- **Ausgabe von Zustandsmeldungen:** Wenn der EVG über ein Display verfügt, müssen darüber auch sicherheitskritische Zustandsmeldungen ausgegeben werden.
- **Schutz von Authentisierungsgeheimnissen:** Wenn der EVG die Eingabe von Authentisierungsgeheimnissen unterstützt (z.B. Eingabe des Administrator-Passworts), muss er diese Geheimnisse geeignet schützen. Der ST-Autor soll in diesem Fall ein entsprechendes EVG-Ziel in das Security Target aufnehmen oder O.Schutz geeignet erweitern.

7.6.4. Betriebssystem als Bestandteil des EVGs (zu Abschnitt 2.3)

Wenn das Betriebssystem Sicherheitsfunktionalität umsetzt, sind folgende Möglichkeiten denkbar:

- Das gesamte Betriebssystem wird als Teil des EVG deklariert. Dies erfordert, dass das **gesamte** Betriebssystem untersucht werden muss und dass diese Untersuchung des Betriebssystems bei Aktualisierungen (Updates, Einspielen von Patches, o.ä.) des Betriebssystems wiederholt werden muss (das Einspielen eines Betriebssystem-**Patches** führt im Allgemeinen zum Verlust des Zertifikats für den Konnektor). Der gesamte **Quellcode** des Betriebssystems muss zur Prüfung vorgelegt werden; dies setzt also die Mitwirkung des Betriebssystem-Herstellers voraus. Die Nutzung bereits evaluierter und zertifizierter Betriebssysteme verspricht nur dann Vorteile, wenn auch genau die gewünschte Sicherheitsfunktionalität evaluiert wurde.
- Diejenigen sicherheitsrelevanten Teile des Betriebssystems, welche vom Netzkonnektor verwendete Sicherheitsfunktionalität umsetzen (z.B. TCP/IP-Stack), werden als Teile des EVGs deklariert. Ein solches Vorgehen setzt voraus, dass entscheidbar ist, in welchen Teilen des Betriebssystems die Sicherheitsfunktionalität implementiert ist. Die **sicherheitsrelevanten** Teile des Quellcodes des Betriebssystems müssen zur Prüfung vorgelegt werden. Wiederholungen der Evaluierung des Betriebssystems (bzw. seiner Teile) sind nur noch dann erforderlich, wenn Aktualisierungen von sicherheitsrelevanten Teilen vorgenommen werden. Ob dieses Vorgehen praktikabel ist, hängt davon ab, wie oft Aktualisierungen erforderlich werden, wie gut die sicherheitsrelevanten Teile **separiert** werden können und wie gut die Auswirkungen von Patches auf die Sicherheitsfunktionalität **analysierbar** sind.
- Die Sicherheitsfunktionalität wird vollständig in der Anwendungssoftware des Netzkonnektors implementiert. Unter Umständen ist es dabei erforderlich, bereits im Betriebssystem vorhandene Funktionalität (z.B. TCP/IP-Stack) erneut zu implementieren. Wenn die Anwendungssoftware ihre Sicherheitsleistung **unabhängig**

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

Zu beachten ist, dass üblicherweise im Rahmen der EVG-Prüfung das Betriebssystem mindestens[84] als IT-Einsatzumgebung mit getestet wird. Es ist im Einzelfall zu entscheiden, wie sich Veränderungen des Betriebssystems auf die Gültigkeit des Zertifikats auswirken.

Anmerkung: Bei Signaturanwendungskomponenten ist die Situation üblicherweise so, dass Software verkauft wird (evtl. in Kombination mit Kartenlesern und Signaturkarten), die zum Einsatz auf (vorhandenen) Standard-PCs vorgesehen ist. Die Software alleine bildet den EVG und Betriebssystem und Hardware die IT-Einsatzumgebung. Es werden Annahmen an das korrekte Funktionieren des Betriebssystems getroffen und durch Tests im Rahmen der Evaluierung des EVG verifiziert; das Zertifikat listet die Plattformen, auf denen der EVG getestet wurde. Im Vergleich dazu kann ein Konnektor aus dedizierter Hardware und Software bestehen, wobei das Betriebssystem des Konnektors Sicherheitsfunktionalität übernehmen kann. In einem solchen Fall muss die vom Betriebssystem übernommene Sicherheitsfunktionalität evaluiert werden.

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

- Wird der EVG z. B. gemeinsam mit einem Betriebssystem ausgeliefert, auf dessen sichere Konfiguration der Anwender keinen Einfluss hat, erscheint es sinnvoll, diese Konfiguration des Betriebssystems im Rahmen der Evaluierung zu betrachten.
- Wird der EVG hingegen auf dem vorhandenen Betriebssystem des Benutzers installiert, liegt dessen sichere Konfiguration in der Verantwortung des Benutzers. Es stellt sich dann jedoch die Frage, ob der Benutzer in der Lage ist, diese Verantwortung wahrzunehmen.

7.6.5. Gemeinsame Nutzung kryptographischer Funktionen (zu Abschnitt 2.4)

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

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

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

evaluierte Funktionalität eines anderen Konnektor-Funktionsblocks nutzt; in diesem Fall umfasst der Composite-EVG beide Funktionsblöcke (Anwendungskonnektor und Netzkonnektor).

7.6.6. Administration des Paketfilters (zu Abschnitt 2.4, Dienst (2) Paketfilter)

Im Normalfall sollte bei der beschriebenen Konstellation (der Paketfilter verwirft alle nicht über den VPN-Tunnel eingehenden Pakete) keine laufende Administration des Paketfilters erforderlich sein. Dennoch wird in diesem Schutzprofil eine Möglichkeit zur Administration vorgesehen (siehe FMT_MSA.1/PF). Falls administrative Eingriffe möglich oder erforderlich sind, sollen alle für eine sichere Administration erforderlichen Hinweise in der Administrator-dokumentation enthalten sein. Im Security Target kann dies durch eine Verfeinerung (Refinement) zu AGD_ADM ausgedrückt werden.

Als Beispiel für die Notwendigkeit der Administration des Paketfilters soll hier der Fall genannt werden, dass ein Netzkonnektor (z.B. auch im Rahmen von Mehrwertdiensten) Verbindungen zu mehreren VPN-Konzentratoren aufbauen können soll, wobei er den (oder die) VPN-Konzentratoren für Anwendungen gemäß § 291 a SGB V strikt von anderen VPN-Konzentratoren separiert (siehe auch Sicherheitsdienst (2) (b) und FPT_SEP.1/VAS). Um weitere VPN-Konzentratoren bekannt zu geben und erreichbar zu machen, kann eine Administration erforderlich werden: Falls sich diese Liste der VPN-Konzentratoren ändert, müssen die Paketfilter-Regeln angepasst werden können.

7.6.7. Physischer Schutz und EVG-Integritätsprüfung (zu Abschnitt 3.6 Annahmen, A.phys_Schutz, zu Abschnitt 4.1.1, O.Schutz und zu Abschnitt 4.2, OE.phys_Schutz)

Das Schutzprofil geht davon aus (A.phys_Schutz), dass die Einsatzumgebung physische Angriffe auf den Konnektor abwehrt.

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

Die genauen Anforderungen zum physischen Schutz des Konnektors durch die Einsatzumgebung sind im Rahmen der Evaluierung zu konkretisieren (betrifft u.a. A.phys_Schutz und OE.phys_Schutz, aber auch O.Schutz). Dabei können sich Auflagen an den Anwender ergeben, die in der Guidance beschrieben werden müssen. Schon im Security Target sollen die speziellen Eigenschaften des konkreten Produkts und die sich daraus ergebenden Anforderungen erläutert werden.

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

Der ST-Autor soll beschreiben, wie der **EVG seine Integrität überprüft** und ob er ggf. auch die Integrität weiterer Komponenten prüft (z.B. zugrundeliegendes Betriebssystem). Falls ein Betriebssystem Sicherheitsfunktionalität umsetzt, gehören zumindest die umsetzenden Teile des Betriebssystems mit zum EVG und ihre Integrität ist dann ebenfalls zu sichern. Siehe auch Abschnitt 7.6.4 *Betriebssystem als Bestandteil des EVGs*.

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

Trotz der Annahme A.phys_Schutz sind Angriffe an der logischen WAN-Schnittstelle auf die im EVG gespeicherten Geheimnisse denkbar (siehe die Liste der Geheimnisse im Unterabschnitt *Sicherer Schlüsselspeicher* des Abschnitts 5.1.1.5). Aus diesem Grund enthält das Schutzprofil die Anforderung **FPT_EMSEC.1**.

Da zum Zeitpunkt der Evaluierung des Produkts (Netzkonnektor) dessen spätere Einsatzumgebung noch nicht bekannt sein wird, wird die Evaluierung stets als Produkt-Evaluierung und nicht als System-Evaluierung[85] durchgeführt werden. Dies impliziert, dass die Erfüllung der Annahmen an die **Einsatzumgebung** nicht an einem (bzw. jedem) konkreten Einsatzort des EVGs überprüft werden..

7.6.8. Denial-of-Service-Angriffe (zu Abschnitt 3.6 Annahmen, A.kein_DoS, und Abschnitt 4.1.3 Ziele für die Paketfilter-Funktionalität, O.PF_LAN)

Der EVG besitzt kaum Möglichkeiten denial-of-service-Angriffe abzuwehren. Der Beitrag des EVG zur Abwehr von denial-of-service-Angriffen besteht lediglich darin, dass nur autorisierten Benutzern Zugang zu den Diensten der Telematikinfrastruktur vermittelt wird. Insofern kann der Netzkonnektor die Abwehr von denial-of-service-Angriffen unterstützen, aber nicht die alleinige Verantwortung dafür übernehmen.

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

Letztlich liegt die Verantwortung für den Schutz der Systeme der zentralen Telematik-infrastruktur jedoch bei den Firewall-Systemen im Perimeter der zentralen Telematikinfra-

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

struktur. Der Schwerpunkt der Abwehr durch den EVG liegt bei den in O.PF_WAN und O.PF_LAN beschriebenen Bedrohungen.

Anfragen zu Mehrwertdiensten, die keinem Fachdienst gemäß § 291 a SGB V zugeordnet sind, laufen nicht über den Anwendungskonnektor (siehe auch A.AK) und werden vom EVG (Netzkonnektor) nicht in das für Fachdienste nach § 291 a SGB V reservierte VPN weitergeleitet.

7.6.9. Korrekte Nutzung des Netzkonnektors (zu Abschnitt 3.6 Annahmen, A.AK)

Das Schutzprofil schließt nicht aus, dass auf einem Primärsystem auch bösartiger Code abläuft (z.B. Trojaner). Der Konnektor muss sich daher gegen Angriffe aus dem Primärnetz ebenfalls schützen (siehe auch die Bedrohungen T.local_TOE_LAN und Application Note 20: LAN-seitiger Paketfilter). Es muss aber, wie unter A.AK formuliert, angenommen werden, dass die Primärsysteme die Dienste des Netzkonnektors korrekt aufrufen, da andernfalls der Konnektor nicht unterscheiden kann, welche Daten mittels VPN übertragen werden sollen (*zu schützende Daten*, z.B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur) und welche nicht.

Hintergrund ist, dass der Netzkonnektor zuverlässig unterscheiden können muss, welche Daten er über das VPN für Anwendungen nach § 291 a SGB V gesichert versenden muss und welche Kommunikation er an diesem VPN vorbei (z.B. in ein anderes VPN für Mehrwertdienste) erlauben kann. Beispielsweise muss der Aufbau des VPN-Kanals unverschlüsselt erfolgen. Mehrwertdienste erfordern möglicherweise Datenkommunikation über ein anderes VPN, welches von den Anwendungen nach § 291 a SGB V getrennt ist. Der ST-Autor soll solche Ausnahmen beschreiben, falls es welche gibt.

Es wird angenommen, dass der Anwendungskonnektor Dokumententypen (z.B. eRezept) korrekt erkennt und unterscheiden kann (technisch wird dies durch Aufruf geeigneter Schnittstellen des Anwendungskonnektors umgesetzt) und auf dieser Basis den Netzkonnektor mit geeigneten Parametern aufruft (wiederum Aufruf über geeignete dedizierte Schnittstellen). Siehe auch Abschnitt 7.6.14.

7.6.10. Sichere Administration des EVGs (zu Abschnitt 3.6, A.Admin_EVG)

Das Recht zur Administration des EVG impliziert die Pflicht, den EVG in sicherer Weise zu administrieren. Das gilt z.B. für das Einstellen von Paketfilter-Filterregeln, falls der EVG diese Möglichkeit bietet. Der ST-Autor soll beschreiben, welche Management-Funktionen (im Sinne der Klasse FMT, siehe Common Criteria, Teil 2 [2]) der EVG bietet.

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

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

Einen hinreichenden Schutz gegen Angreifer, welche gefälschte Konnektoren in Umlauf bringen, stellen ein geeignetes Auslieferungsverfahren (**ADO_DEL.2**) sowie sichere Verfahren zur Inbetriebnahme (**ADO_IGS.1**) dar, sofern sie mit weiteren Maßnahmen

kombiniert werden, welche spätere Veränderungen am Konnektor mit Sicherheit ausschließen oder hinreichend erkennbar machen, z.B. Aufbewahrung in einem gesicherten Bereich.

Der Netzkonnektor muss auf Anforderung seine Authentizität nachweisen, indem er beispielsweise ein sicheres Authentisierungsprotokoll implementiert. Das dafür erforderliche Geheimnis kann er dem SM-K entnehmen.

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

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

Der Zufallszahlengenerator kann theoretisch auch durch eine SMC Typ B realisiert werden. Falls die Zufallszahlen für den Netzkonnektor von einer dem Anwendungskonnektor zugeordneten SMC Typ B bezogen werden, muss dann aber sichergestellt werden, dass die Zufallszahlen auf dem Kanal zwischen Anwendungskonnektor und Netzkonnektor nicht manipuliert werden.

Es kann sinnvoll sein, den gleichen Zufallszahlengenerator von verschiedenen Teilkomponenten des Konnektors (Netzkonnektor, Anwendungskonnektor) zu nutzen – etwa wenn das SM-K über keinen geprüften Zufallszahlengenerator verfügt. Dies setzt im Falle einer Mehrbox-Lösung (siehe Application Note 6: Einbox- vs. Mehrbox-Lösung) aber voraus, dass die einzelnen Teilkomponenten sicher miteinander kommunizieren (organisatorischer Schutz wie von A.phys_Schutz gefordert oder technischer Schutz durch sicheren Kanal und vorherige gegenseitige Authentisierung) und geeignete Schnittstellen für die gemeinsame Nutzung von Ressourcen (z.B. Chipkarten) bereitstellen. Der ST-Autor soll dies bei der Formulierung des Security Targets geeignet berücksichtigen.

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

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

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

Siehe auch Abschnitte 4.2.1.1 *Anforderungen an den Konnektor (normativ) / Nicht-funktionale Anforderungen / Konnektoridentität / Ausführung* und 4.2.1.2 ... */ Bedeutung für den Konnektor* der Konnektor-Spezifikation [20] (Version 2.0.0). Dort heißt es u.a.:

„[4.2.1.1] *Grundsätzlich MUSS der Schlüssel zur Geräteidentität in einem sicheren Schlüsselspeicher hinterlegt sein. Dieser Schlüsselspeicher wird SM-K genannt. Die SM-K MUSS dabei: (1) den privaten Schlüssel sicher schützen, d. h., dass sie den privaten Schlüssel*

NICHT herausgeben DARF und dabei auch physikalischen Angriffen widerstehen MUSS (Tamper Resistance), [...]

[4.2.1.2] [...] *Zudem muss die SM-K sicher mit dem Gerät verbunden sein. Die sichere Verbundenheit zwischen Schlüsselspeicher und Konnektor MUSS durch technische und / oder organisatorische Maßnahmen sichergestellt werden. Kann ein Betreiber, z. B. ein Krankenhaus, durch zertifizierbare organisatorische Regeln für die Integrität des Konnektors garantieren, können Mehrkomponentenkonnektoren eingesetzt werden, in denen die Geräteidentität in einem separaten Schlüsselspeicher (z. B. Hardware Security Module (HSM)) hinterlegt ist."*

7.6.14. Datenkennzeichnung durch Anwendungskonnektor (zu Abschnitt 4.2 Sicherheitsziele für die Umgebung, OE.AK)

Ob Daten *zu schützende Daten* im Sinne des § 291 a SGB V sind, wird durch die Primärsysteme bestimmt. Die „Kennzeichnung" solcher Daten erfolgt daher zunächst im Primärsystem durch den Aufruf einer geeigneten Schnittstelle des Anwendungskonnektors (sinngemäß z.B. „eRezept einstellen") und die Verwendung eines standardisierten Dokumententyps (z.B. XML-Schemaprüfung). Der Anwendungskonnektor muss diese Datenkennzeichnung an den Netzkonnektor weiterleiten, was wiederum durch den Aufruf geeigneter Schnittstellen erfolgt. Technisch erfolgt die „Kennzeichnung" also nicht durch das Setzen von Sicherheitsattributen der zu schützenden Daten, sondern dadurch, dass bei der Übergabe der Daten geeignete Schnittstellen aufgerufen werden (siehe auch Abschnitt 7.6.9).

In diesem Sinne vom Anwendungskonnektor als *zu schützende Daten* gekennzeichnete Daten (Daten für Anwendungen gemäß § 291 a SGB V) dürfen vom EVG (Netzkonnektor) ausschließlich gesichert, das heißt über den entsprechenden VPN-Tunnel für Dienste gemäß § 291 a SGB V, an die zentrale Telematikinfrastruktur weitergeleitet werden (an *VPN-Konzentratoren für Dienste gemäß § 291 a SGB V*).

Es ist denkbar, dass der EVG (Netzkonnektor) im Rahmen von Mehrwertdiensten weitere VPN-Tunnel zu anderen *VPN-Konzentratoren für Mehrwertdienste* unterhält. Dabei ist es wichtig, dass der EVG eine konsequente Trennung von *zu schützenden Daten* gemäß § 291 a SGB V und Daten für Mehrwertdienste durchsetzt. Siehe auch den Aspekt „Informationsflusskontrolle" in Abschnitt 5.1.1.1 sowie FDP_IFC.1/PF in Abschnitt 5.1.1.2 sowie Abschnitt 7.6.15.

7.6.15. Arten von VPN-Konzentratoren (zu Abschnitt 2.4 Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste, Dienst (2) (b) Separationsmechanismen für Mehrwertdienste)

Arten von VPN-Konzentratoren: Der Netzkonnektor erlaubt WAN-seitig nur Verbindungen zu VPN-Konzentratoren sowie die für den Verbindungsaufbau zu den VPN-Konzentratoren erforderlichen direkten Internet-Zugriffe (u.a.: DNS-Abfragen und IPsec-Protokoll für VPN-Aufbau, ferner evtl. Bezug von Sperrlisten (CRLs) für Zertifikatsprüfungen; für Details siehe die Konnektor-Spezifikation [20], v2.0.0, Abschnitt 3.8.2). Das heißt, es ist von diesen Ausnahmen abgesehen keine direkte ausgehende Verbindung ins Transportnetz (z.B. Internet) möglich. Aus der Menge aller VPN-Konzentratoren, mit denen der Netzkonnektor Verbindungen aufbauen kann, sind einer oder einige dadurch ausgezeichnet, dass sie den

Zugang zur Telematikinfrastruktur (für Dienste gemäß § 291 a SGB V) bereitstellen. Diese werden als *VPN-Konzentratoren für Dienste gemäß § 291 a SGB V* bezeichnet. Weitere VPN-Konzentratoren werden als *VPN-Konzentratoren für Mehrwertdienste* bezeichnet.

Der Netzkonnektor separiert Informationsflüsse über *VPN-Konzentratoren für Dienste gemäß § 291 a SGB V* streng von anderen Informationsflüssen (z.B. Mehrwertdiensten). Der Netzkonnektor kann für den Zugriff auf Mehrwertdienste weitere VPN-Verbindungen zu anderen *VPN-Konzentratoren für Mehrwertdienste* aufbauen. *VPN-Konzentratoren für Mehrwertdienste* dürfen keine Verbindung zur Telematikinfrastruktur für Dienste gemäß § 291 a SGB V haben. Hinter den *VPN-Konzentratoren für Mehrwertdienste* werden durch Proxys gesicherte und vermittelte Mehrwertdienste angeboten. Dabei wird angenommen, dass diese Proxys eine Schädigung des LANs des Leistungserbringers effektiv abwehren. Mehrwertdienste können nur über *VPN-Konzentratoren für Mehrwertdienste* und solche Proxies genutzt werden. Diese Architektur ermöglicht eine handhabbare und sichere Konfiguration des Paketfilters im Netzkonnektor. Der EVG baut die VPN-Kanäle selbständig auf und akzeptiert keine eingehenden Verbindungsversuche.

Es ist denkbar, dass ein Leistungserbringer (z.B. große Klinik), der zusätzlich Internet-Zugang in seinen Geschäftsräumen haben will, über eine entsprechend sichere Firewall einen weiteren, vom Konnektor unabhängigen Internet-Zugang bereitstellt oder aber einen vom Praxis-LAN getrennten zusätzlichen PC für Anwendungen wie E-Mail verwendet. Dann trägt jedoch der Leistungserbringer und nicht der Konnektor die Verantwortung für die Sicherheit dieses Zugangs. Bei Mehrkomponentenlösungen oder dem Wunsch nach einer Anbindung des gesamten lokalen Netzes ist der Zulassungsprozess der gematik zu beachten. Der ST-Autor soll beschreiben, welche Funktionalität genau der EVG bietet.

7.6.16. Sichere Kanäle

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

Neben dem sicheren VPN-Tunnel zum VPN-Konzentrator sind sichere Kanäle zu folgenden dezentralen Komponenten denkbar:

- SM-K (falls sich diese nicht im Gehäuse des Konnektors befindet, siehe Application Note 60:),
- Anwendungskonnektor (im Falle von Mehrbox-Lösungen, siehe Application Note 6:),
- lokale Administration (falls der Schutz gegen Abhören von Authentisierungsdaten und die Manipulation von administrativen Kommando- und Antwortnachrichten nicht durch die Umgebung geleistet wird),
- zentrale Administration (optional),
- sicheres Software-Update.

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

- gegenseitige Authentisierung der Enden des sicheren Kanals über Zertifikate,
- Sicherung der Vertraulichkeit der übertragenen Daten (Verschlüsselung) und

- Sicherung der Integrität der übertragenen Daten (Signatur oder MAC-Bildung).

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

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

7.6.17. Emanation Security (zu Abschnitt 5.1.1.5, FPT_EMSEC.1)

Die privaten Authentisierungsschlüssel für die VPN-Verbindung werden im SM-K gespeichert und angewendet, so dass keine Berechnung innerhalb des EVG stattfindet. Im Rahmen der Authentisierung der VPN-Kommunikationspartner wird aber ein Sitzungsschlüssel (session key) abgeleitet, der vom EVG geschützt werden muss, da seine Kompromittierung z.B. einem Angreifer aus dem Internet Zugriff auf das LAN des Leistungserbringers ermöglichen kann.

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

Falls Software-Updates in verschlüsselter Form übertragen werden, muss der EVG die Vertraulichkeit des Schlüsselmaterials (geheimer symmetrischer oder privater asymmetrischer Schlüssel) schützen, mit dem empfangene Software-Updates entschlüsselt werden. Falls Software-Updates unverschlüsselt übertragen werden, darf in der Zeile „key material used to decrypt encrypted software updates (if applicable)“ in FPT_EMSEC.1.1 im Security Target die Zuweisung „none“ gewählt werden.

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

Die Anforderung FPT_EMSEC.1.1 erzwingt nicht notwendigerweise Penetrationstests, sondern es ist auch denkbar, dass ein Aspekt durch argumentative Nachweise abgedeckt wird. Beispielsweise kann im Rahmen einer Quellcodeanalyse nachgewiesen werden, dass bei einer

PIN-Prüfung keine zeitlichen Abhängigkeiten bestehen, die für Angriffe ausgenutzt werden können.

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

7.6.18. Erläuterung zur Auswahl und Verfeinerung der Komponente FPT_ITI.1/Update (zu Abschnitt 5.1.1.6)

In der Anforderung FPT_ITI.1/Update muss der EVG die Integrität von TSF-Daten beim Import nachprüfen (z.B. durch das Verifizieren der Signatur beim Import von signierten Daten). Nachdem die gewünschte funktionale Anforderung in CC Teil 2 [2] so nicht exakt enthalten war, die Anforderung FPT_ITI.1 dem Wortlaut nach aber durchaus verwendet werden kann, wurde FPT_ITI.1/Update so verfeinert (refinement), dass auf die Definition einer explizit definierten Anforderung verzichtet werden konnte. Im Folgenden werden weitere Gründe aufgezählt, diesen Ansatz zu wählen.

CC Teil 2 [2] formuliert in Paragraph 381 und 382:

> *This family defines the rules for the protection, from unauthorised modification, of TSF data during transmission between the TSF and a remote trusted IT product. This data could, for example, be TSF critical data such as passwords, keys, audit data, or TSF executable code.*
>
> *FPT_ITI.1 Inter-TSF detection of modification, provides the ability to detect modification of TSF data during transmission between the TSF and a remote trusted IT product, under the assumption that the remote trusted IT product is cognisant of the mechanism used.*

Aus diesen Formulierungen wird deutlich, dass die Komponente dazu verwendet werden können soll, um den Schutz vor Modifikationen (z.B. durch eine Signatur) bei der Übertragung von Daten zwischen dem EVG und einem externen vertrauenswürdigen IT-Produkt (z.B. ein zentraler Dienst, welcher Software-Updates verteilt) zu fordern.

Bei den übertragenen Daten handelt es sich um TSF-Daten. Ausführbarer Code (TSF executable code) wird explizit als Beispiel genannt. Da ausführbarer Code TSF-Daten darstellt, sollte bei der Auswahl einer funktionalen Sicherheitsanforderung eine Anforderung aus der Klasse FPT, nicht jedoch aus der Klasse FDP ausgewählt werden.

Aus der Formulierung sowohl der einleitenden Texte (Paragraph 381 und 382) als auch der Komponente FPT_ITI.1 selbst wird keine Richtung deutlich („*between A and B*“ impliziert nicht die Richtung „*from A to B*“). Somit ist der Einsatz Komponente FPT_ITI.1 nicht auf die Erzeugung einer Signatur beim Export von Daten beschränkt, sondern kann auch – wie im vorliegenden Fall – auf die Überprüfung einer Signatur beim Import von Daten angewendet werden.

Zwar wird in der Überschrift der Familie FPT_ITI („Integrity of exported TSF data“) durch die Verwendung des Begriffs „Export“ eine Richtung suggeriert. Da aber der CC Teil 2 [2]

eine zugehörige komplementäre Anforderung „Import“ nicht enthält, ist davon auszugehen, dass es sich bei dieser Verwendung des Begriffs „Export“ um ein Versehen handelt.

7.6.19. LAN-seitiger Paketfilter (zu Abschnitt 3.6, A.PF_LAN sowie zu Abschnitt 4.1.3 O.PF_LAN und zu Abschnitt 4.2 OE.PF_LAN)

Der Netzkonnektor (EVG) verfügt grundsätzlich immer über einen LAN-seitigen Paketfilter, der den Netzkonnektor vor potentiellen Angriffen aus dem LAN schützt. Im Fall einer Einbox-Lösung soll dieser LAN-seitige Paketfilter des Netzkonnektors auch den Anwendungskonnektor schützen (vgl. Abbildung 3 in Abschnitt 2.1 Einsatzumgebung des Konnektors). Im Fall einer Mehrkomponentenlösung sind Topologien denkbar, bei denen der Netzkonnektor dies nicht leisten kann (vgl. etwa Abbildung 2 im gleichen Abschnitt 2.1). Daher wird im Fall einer Mehrkomponentenlösung gefordert, dass die IT-Einsatzumgebung einen LAN-seitigen Paketfilter für den Anwendungskonnektor bereitstellen soll.

Im Schutzprofil wird diese Tatsache durch die Annahme **A.PF_LAN,** das Umgebungsziel **OE.PF_LAN** und schließlich die Anforderung **FDP_IFC.1/Env** modelliert; diese Elemente fordern im Fall der Mehrkomponentenlösung den erforderlichen Schutz durch einen LAN-seitigen Paketfilter von der IT-Einsatzumgebung. Das EVG-Ziel **O.PF_LAN** beschränkt sich (vor dem Hintergrund der Mehrkomponentenlösung) darauf, dass sich der EVG selbst mit Hilfe seines LAN-seitigen Paketfilters vor potentiellen Angriffen aus dem LAN schützt.

Im Fall einer Einbox-Lösung sind daher Anpassungen an diesen Elementen der Sicherheitspolitik erforderlich: Der Netzkonnektor muss im Fall einer Einbox-Lösung den Schutz des Anwendungskonnektor mit übernehmen. Daher ist in diesem Fall die Annahme **A.PF_LAN** durch eine entsprechende Bedrohung zu ersetzen und das Ziel **O.PF_LAN** ist zu erweitern (der Netzkonnektor muss nicht nur sich selbst, sondern auch den Anwendungskonnektor vor potentiellen Angriffen aus dem LAN schützen) und auch **FDP_IFF.1/PF** ist geeignet zu ergänzen. Gleichzeitig entfällt die Notwendigkeit für die Annahme **A.PF_LAN** und das Umgebungsziel **OE.PF_LAN** sowie für die Anforderung **FDP_IFC.1/Env**. Der ST-Autor soll daher im Fall einer Einbox-Lösung A.PF_LAN, OE.PF_LAN und FDP_IFC.1/Env (bzw. den gesamten Abschnitt 5.2.4) ersatzlos streichen und die Erklärungsteile (Rationale) entsprechend anpassen.

7.6.20. Bedrohungen (zu den Abschnitten 3.4.2.1 T.local_TOE_LAN und folgenden sowie zu den Abschnitten 6.1.2.1 T.local_TOE_LAN und folgenden)

Da der EVG (Netzkonnektor) im Fall einer Einbox-Lösung mit seinem LAN-seitigen Paketfilter auch den Anwendungskonnektor im weiteren Sinne[86] schützt,

- umfasst die Bedrohung T.local_TOE_LAN in Abschnitt 3.4.2.1 im Fall einer Einbox-Lösung auch LAN-seitige Angriffe auf den Anwendungskonnektor. Der ST-Autor soll prüfen, ob in der Formulierung der Bedrohung T.local_TOE_LAN ggf. der Begriff „Konnektor“ statt „Netzkonnektor“ verwendet werden kann bzw. sollte. Im Erklärungsteil in Abschnitt 6.1.2.1 muss der ST-Autor dann in Übereinstimmung mit

[86] Im Rest dieses Abschnitts bezieht sich der Begriff „Anwendungskonnektor“ stets auf den „Anwendungskonnektor im weiteren Sinne“.

Abschnitt 3.4.2.1 prüfen, ob die Angriffe sich ausschließlich gegen den EVG (Netzkonnektor) richten oder ob Angriffe gegen den Konnektor allgemein betrachtet und abgewehrt werden. Abhängig davon muss der ST-Autor den Erklärungsteil entsprechend anpassen; im ST sollte der Erklärungsteil keine Fallunterscheidungen mehr enthalten.

Das gleiche gilt sinngemäß auch für weitere Bedrohungen (in den Abschnitten 3.4.2.2 T.remote_TOE_WAN und folgende) sowie für die zugehörigen Erklärungsteile (in den Abschnitten 6.1.2.2 und folgende), die ggf. durch den ST-Autor anzupassen sind:

- Zur Bedrohung T.remote_TOE_WAN (Abschnitt 3.4.2.2) ist anzumerken: Der Netzkonnektor schützt nicht nur sich selbst, sondern auch den Anwendungskonnektor. Deshalb werden in dieser Bedrohung ganz allgemein Angriffe auf den „Konnektor“ betrachtet. Gleiches gilt für die Bedrohung T.remote_TOE_LAN (Abschnitt 3.4.2.3).
- Zur Bedrohung T.remote_VPN_Data (Abschnitt 3.4.2.4) ist anzumerken: Der Netzkonnektor schützt die Kommunikation zwischen Anwendungskonnektor und zentraler Telematikinfrastruktur. Angriffe aus dem WAN richten sich jedoch stets gegen den Netzkonnektor.
- In analoger Weise wurden die Begriffe „Netzkonnektor“ und „Konnektor“ in der Formulierung der Bedrohungen T.local_admin_LAN und T.remote_admin_WAN (Abschnitte 3.4.2.5 und 3.4.2.6) verwendet und sind ggf. vom ST-Autor geeignet anzupassen.
- Zur Bedrohung T.counterfeit (Abschnitt 3.4.2.7) ist anzumerken: Im Fall einer Einbox-Lösung ist die Tatsache, dass ein Angreifer gefälschte Netzkonnektoren in Umlauf bringt, gleichbedeutend mit dem In-Umlauf-Bringen gefälschter Konnektoren.

7.7. Literaturverzeichnis

7.7.1. Kriterien

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Version 2.3, August 2005, CCMB-2005-08-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

Hinweis: Die Common Criteria und die zugehörige CEM sind unter http://www.commoncriteriaportal.org/, Stichworte „Experts“ / „Official CC/CEM versions“ veröffentlicht.

Die Common Criteria Version 2.3 wurden im Bundesanzeiger Ausgabe Nr. 95 vom 19.05.2006 auf Seite 3730 durch das Bundesministerium des Inneren veröffentlicht (siehe auch http://www.bundesanzeiger.de/old/banz/banzinha/BAnz_58_095.htm).

7.7.2. Gesetze und Verordnungen

[5] 5. Sozialgesetzbuch (SGB V), Gesetzliche Krankenversicherung, Artikel 1 des Gesetzes vom 20. Dezember 1988 (BGBl. I S. 2477)

[6] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[7] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (deutsches Signaturgesetz – SigG 2001; BGBI. I S.876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)

[8] Verordnung zur elektronischen Signatur (deutsche Signaturverordnung – SigV 2001) vom 16.November 2001 (BGBl. I S. 3074), geändert durch Artikel 2 des Gesetzes vom 4. Januar 2005 (BGBl. I S. 2)

[9] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 22. Februar 2007, veröffentlicht am 12. April 2007 im Bundesanzeiger Nr. 69, Seite 3759, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[10] Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)

7.7.3. Schutzprofile (Protection Profiles) und Technische Richtlinien

[11] Common Criteria Protection Profile electronic Health Card (eHC) / elektronische Gesundheitskarte (eGK), Version 1.02, 12.12.2005, BSI-PP-0020, Bundesamt für Sicherheit in der Informationstechnik

[12] Common Criteria Protection Profile Health Professional Card (HPC) / Heilberufsausweis (HBA), Version 1.0, 12.12.2005, BSI-PP-0018, Bundesamt für Sicherheit in der Informationstechnik

[13] Common Criteria Protection Profile Secure Module Card (PP-SMC), Version 1.0, 01.02.2006, BSI-PP-0019, Bundesamt für Sicherheit in der Informationstechnik

[14] Common Criteria Protection Profile – Secure Signature-Creation Device (SSCD) Type 3, CEN/ISSS by ESIGN Workshop – Expert Group F, Version 1.05, 25 July 2001, registered as BSI-PP-0006-2002

[15] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart (European Smart Card Industry Association), developed by Atmel Smart Card ICs,

Hitachi Europe Ltd., Infineon Technologies AG, Philips Semiconductors, registered as BSI-PP-0002-2001

[16] Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116), Version 1.0, 23.03.2007, Technische Arbeitsgruppe TR-03116

7.7.4. Verwandte Spezifikationen und Arbeiten aus Vorprojekten

[17] Einführung der Gesundheitskarte: Konnektorspezifikation, Teil 1: Allgemeine Funktionen und Schnittstellen des Konnektors, Version 0.6.1 („0.6.0“), 27.09.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[18] Einführung der Gesundheitskarte: Konnektorspezifikation, Teil 1: Allgemeine Funktionen und Schnittstellen des Konnektors, Version 0.9.0, 27.12.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[19] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec Kon], Version 1.0.0, 02.03.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[20] Einführung der Gesundheitskarte: Konnektorspezifikation [gemSpec Kon], Version 2.0.0, 04.05.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[21] Gesamtarchitektur mit Stand vom 15.09.2006, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), veröffentlicht als „Bekanntmachung der Gesamtarchitektur und der Richtlinie für den Betrieb der Gesundheitstelematik nach § 3 Abs. 4 Satz 1 und § 5a Abs. 1 Satz 2 der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte vom Oktober 2006“, Bundesministerium für Gesundheit (BMG)

[22] Einführung der Gesundheitskarte: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpecKrypt], Version 0.9.1 (freigegeben), 15.05.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[23] Einführung der Gesundheitskarte: Netzwerkspezifikation [gemNet], Version 1.0.0, 16.06.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[24] Einführung der Gesundheitskarte: Spezifikation Netzwerksicherheit [gemNetSich], Version 1.0.0, 23.02.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[25] Basisarchitektur für Testvorhaben, Gesamtarchitektur, Rahmenbedingungen, Version 0.8 Draft, 19.12.2005, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) mit Anhang und Erläuterungen (ebenfalls Version 0.8 vom 19.12.2005)

[26] Einführung der Gesundheitskarte: Sicherheitskonzept (Konnektor), Version 0.0.2, 15.03.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[27] Einführung der Gesundheitskarte: Sicherheitskonzept – Offline, Version 1.0.0, 18.05.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[28] Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, Erste Fassung der Spezifikation, Version 1.0, 14.03.2005, Projektgruppe FuE-Projekt „Lösungsarchitektur“ der Fraunhofer-Institute ISST, IAO und SIT, gefördert durch das BMGS

[29] Einführung der Gesundheitskarte: Spezifikation eHealth-Kartenterminal, Version 1.2.0, 16.10.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[30] Einführung der Gesundheitskarte: Spezifikation Infrastrukturkomponenten: Zeitdienst, Version 0.9.0, 30.05.2006, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[31] Einführung der Gesundheitskarte: Glossar, Version 1.7.0, 30.03.2007, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

7.7.5. Standards

7.7.5.1. IETF, RFCs

[32] J. Burbank, J. Martin: The Network Time Protocol (NTP) Version 4 Protocol Specification, March 2006, http://www.ietf.org/internet-drafts/draft-ietf-ntp-ntpv4-proto-02.txt

[33] D. Mills: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, January 2006, RFC 4330 (SNTP), http://www.rfc-editor.org/rfc/rfc4330.txt

IPsec, AH, ESP, IKE

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

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

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

[37] D. Harkins, D. Carrel: The Internet Key Exchange (IKE), November 1998, RFC 2409 (IKE v1), http://www.ietf.org/rfc/rfc2409.txt

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

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

[40] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg (January 2005): RFC 3948, UDP Encapsulation of IPsec ESP Packets, http://www.rfc-editor.org/rfc/rfc3948.txt

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

SSL, TLS

[42] Alan O. Freier, Philip Karlton, Paul C. Kocher: The SSL Protocol Version 3.0, 18.11.1996, Internet Draft, http://wp.netscape.com/eng/ssl3/draft302.txt

[43] T. Dierks, C. Allen: The TLS Protocol Version 1.0, January 1999, RFC 2246, http://www.ietf.org/rfc/rfc2246.txt

[44] R. Khare, S. Lawrence: Upgrading to TLS Within HTTP/1.1, May 2000, RFC 2817, http://www.ietf.org/rfc/rfc2817.txt

[45] E. Rescorla: HTTP Over TLS, May 2000, RFC 2818, http://www.ietf.org/rfc/rfc2818.txt

[46] P. Chown: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002, RFC 3268, http://www.ietf.org/rfc/rfc3268.txt

[47] B. Adoba, D. Simon: PPP EAP TLS Authentication Protocol, October 1999, RFC 2716, http://www.ietf.org/rfc/rfc2716.txt

7.7.5.2. NIST/FIPS

[48] Data Encryption Standard (DES), Federal Information Processing Standards Publication FIPS PUB 46-3, reaffirmed 25.10.1999, U. S. Department of commerce, National Institute of Standards and Technology (NIST)

[49] Secure Hash Standard (SHA), Federal Information Processing Standards Publication FIPS PUB 180-2, 01.08.2002, U. S. Department of commerce, National Institute of Standards and Technology (NIST)

[50] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication FIPS PUB 197, 26.11.2001, U. S. Department of commerce, National Institute of Standards and Technology (NIST)

7.7.5.3. PKCS

[51] PKCS #1: RSA Encryption Standard, version 1.5 (PKCS#1, Version 1.5), RSA Laboratories, revised 01.11.1993

[52] PKCS #1 v2.0: RSA Cryptography Standard (PKCS #1, Version 2.0), RSA Laboratories, 01.10.1998

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

[54] PKCS #7: Cryptographic Message Syntax Standard, version 1.5 (PKCS#7, Version 1.5), RSA Laboratories, revised 01.11.1993

7.7.5.4. ISO/IEC

[55] ISO/IEC 7816-4:2005 Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange

7.7.5.5. Andere Standards

[56] W3C Recommendation: XML-Signature Syntax and Processing, 12.02.2002, World Wide Web consortium (W3C), http://www.w3.org/TR/xmldsig-core/

7.7.6. Weiterführende Literatur

[57] BSI Firewall Studie II, erstellt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI), Abschlussdokument vom 18.05.2001 (siehe http://www.bsi.bund.de/literat/studien/firewall/fwstud.htm)

[58] Cheswick, W. R., Belovin, S. M.: Firewalls and Internet Security, Addison-Wesley, 1994