Security Target für secunet konnektor 2.0.0

(eHealth Konnektor PTV5 WR1)

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

Änderungsverlauf

Version	Datum	Änderungen	Anmerkungen
1.0	26.04.2022	Initial Version	Initiale Version basierend auf dem PTV5 ST (BSI-DSZ-CC-1184-2022), Version 2.3 vom 03.03.2022
1.1	15.06.2022	Anpassen des ST an zertifiziertes PP0098 (BSI-DSZ-CC-0098-V3-2021-MA-01), v1.6 vom 30.03.2022	-
1.2	27.06.2022	Errata ergänzt und Direktiven aktualisiert	-

Letzte Version: 1.2 (27.06.2022)

Inhaltsverzeichnis

1. ST-Einführung

1.1. ST-Referenz

Titel:	Security Target für secunet konnektor 2.0.0
Version des Dokuments:	1.2
Datum des Dokuments:	27.06.2022
Allgemeiner Status:	Version zur Evaluierung
ST-Registrierung:	BSI-DSZ-CC-1201
PP Registrierung:	BSI-CC-PP-0098, 1.6
PP Registrierung bei:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC-Version	3.1 (Revision 5)
Vertrauenswürdigkeitsstufe:	EAL3 erweitert um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2
Verfasser:	SRC GmbH und secunet Security Networks AG
TOE Name.	secunet konnektor 2.0.0
TOE Version	5.1.2:2.0.0
Ausbaustufe	PTV5 WR1

Dieses Security Target wurde konform zu den folgenden Dokumenten

[4] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

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

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

und unter Berücksichtigung

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

erstellt. Darüber hinaus orientiert sich dieses Dokument in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang in Abschnitt 9.6 (insbesondere Abschnitt 9.6.4) aufgeführt sind; allen voran die Konnektorspezifikation:

[27] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon], PTV5: Version 5.15.0, 31.01.2022, gematik GmbH

1.2. ST-Übersicht

Dieses Security Target beschreibt den Schutzbedarf für den Konnektor secunet konnektor 2.0.0 gemäß Spezifikation [27].

Der Konnektor besteht aus dem Netzkonnektor (NK) und dem Anwendungskonnektor (AK) und verwendet die Security Module Card Konnektor (gSMC-K). Der Konnektor stellt die Plattform für die Ausführung von Fachmodulen bereit.

- Der Netzkonnektor stellt Paketfilter- und VPN-Funktionalität für die Kommunikation mit der zentralen Telematikinfrastruktur-Plattform und einem Sicheren Internet Service (SIS) bereit, ebenso die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und fachanwendungsspezifischen Diensten (Fachdiensten bzw. Intermediären). Darüber hinaus verwendet er die Hardware-Virtualisierung der CPU, um dem AK und seinen Fachmodulen einen Separationsmechanismus zur Verfügung zu stellen.

- Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssytem und dem Objektsystem für gSMC-K. Sie speichert Schlüsselmaterial für den Netzkonnektor und den Anwendungskonnektor und stellt kryptographische Sicherheitsfunktionen bereit.

- Die Sicherheitsfunktionalität des Anwendungskonnektors umfasst die Signaturanwendung, die Verschlüsselung und Entschlüsselung von Dokumenten, den Kartenterminaldienst und den Chipkartendienst. Zusammen mit dem Netzkonnektor ermöglicht der Anwendungskonnektor zudem die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und Fachdiensten.

1.2.1. Abgrenzung

Das Schutzprofil BSI-CC-PP-0098 [16] definiert die Sicherheitsanforderungen an den Konnektor, bestehend aus Netzkonnektor und Anwendungskonnektor. Die gSMC-K ist nicht Teil des EVG und wird separat betrachtet: Das Chipkartenbetriebssytem der gSMC-K ist von der gematik zugelassen (A.AK.gSMC-K). Für das Chipkartenbetriebssystem existiert eine eigene Spezifikation [31].

Der EVG des vorliegenden ST schließt die gSMC-K als Teil der IT-Umgebung ein. Die relevanten Sicherheitsziele der Einsatzumgebung, wie OE.NK.gSMC-K, OE.NK.KeyStorage und OE.NK.RNG beziehen sich auf die Funktionalität der gSMC-K.

1.2.2. Terminologie

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

Der Konnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens und den Clientsystemen der Leistungserbringer. Die Chipkarten elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA), die Institutionskarte (SMC-B, Security Module Card Typ B), die SMC-B der Gesellschafterorganisationen (SMC-B ORG),

das Hardware-Sicherheitsmodul HSM-B, die Kartenterminals und die Konnektoren bilden die dezentralen Komponenten der Telematikinfrastruktur. Zu den Clientsystemen gehören die Praxisverwaltungssysteme der Ärzte (PVS), die Krankenhausinformationssysteme (KIS) und die Apothekenverwaltungssysteme (AVS). Der Konnektor stellt auch eine gesicherte Verbindung zu einem Sicheren Internet Service (SIS) bereit. Der Konnektor unterstützt weiterhin die Vorläuferkarten des HBA, den HBA-qSig und den ZOD-2.0.

1.3. EVG-Beschreibung

Der Evaluierungsgegenstand ist:

- der Konnektor, secunet konnektor 2.0.0 bestehend aus den Komponenten
    - Netzkonnektor,
    - Anwendungskonnektor,
    - Fachmodul „Versichertenstammdatenmanagement“ (VSDM) [37].

welcher als eine **Einbox-Lösung** implementiert wird.

Der EVG secunet konnektor 2.0.0 umfasst die Software des Konnektors und die dazugehörige Dokumentation für Administratoren und Benutzer [110], [111] [112] und [116].

Komponenten des Konnektors	Version
Hardware (nicht Teil des EVG)	2.0.0
BIOS FW (nicht Teil des EVG)	CSASR007, CSASR009 oder CSASR011
Fachmodul AMTS (nicht Teil des EVG)	5.1.1
Fachmodul NFDM (nicht Teil des EVG)	5.1.1
Fachmodul ePA (nicht Teil des EVG)	5.1.1
Softwareversion Netzkonnektor[1]	5.1.2
Softwareversion Anwendungskonnektor (inkl. Fachmodul VSDM)	5.1.2
Bedienhandbuch	6.1
Errata Bedienhandbuch	1.0
Hinweise und Prüfpunkte für Endnutzer	1.8
REST-API Spezifikation	5.0.0
Security Guidance Fachmodulentwicklung	1.5

Tabelle 1: Komponenten der Einbox-Lösung

[1] Mit dieser Versionsnummer ist auch die Version des Anwendungskonnektors fest bestimmt. Zur exakten bestimmung der TOE Version reicht daher die Angabe der Softwareversion des Netzkonnektor.

1.3.1. EVG-Typ

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

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

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

Die Sicherheitsfunktionalität

- einer Firewall,
- eines VPN-Clients,
- von Servern für Zeitdienst, Namensdienst und DHCP-Dienst, und
- die Basisdienste zum Aufbau von TLS-Kanälen[2],

werden durch den Bestandteil Netzkonnektor erbracht (**Teil des EVG**).

Die Sicherheitsfunktionalität

- einer Signaturanwendung,
- eines Kryptomoduls für die Verschlüsselung und für die Initiierung der gesicherten Kommunikation zwischen dem Konnektor und dem Clientsystem, zwischen Fachmodulen und Fachdiensten sowie zwischen Servern und dem Kartenterminaldienst, dem Chipkartendienst

werden durch den Anwendungskonnektors erbracht (**Teil des EVG**).

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

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

[2] Die Basisdienste zum Aufbau von TLS-Kanälen werden vom Anwendungskonnektor implementiert sind aber formal dem Netzkonnektor zugeordnet.

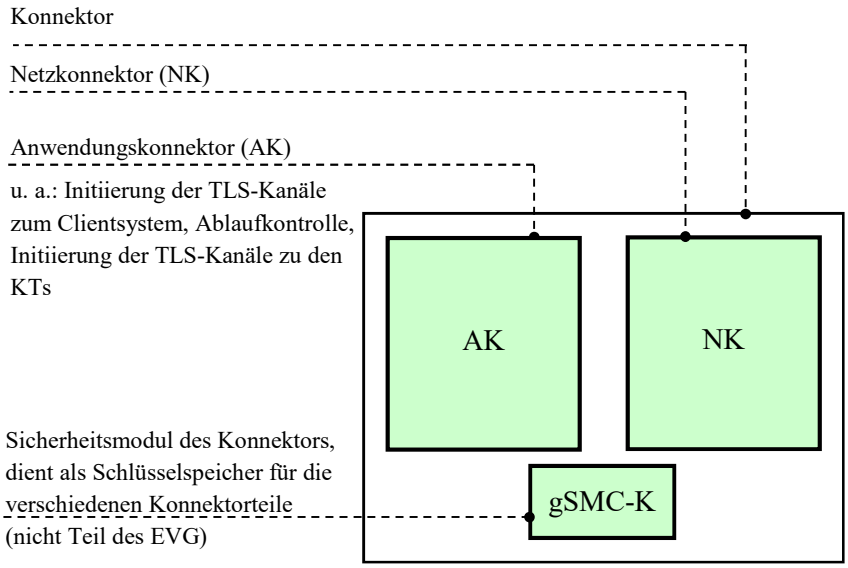

Abbildung 1: Funktionsblöcke des Konnektors

1.3.1.1. Sicherheitsfunktionen des Netzkonnektors (NK)

Firewall

Der Netzkonnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens (außerhalb der Verantwortlichkeit der Leistungserbringer) und den dezentralen Systemen. Er stellt den netzseitigen Abschluss der zentralen Telematikinfrastruktur-Plattform dar. Der Zugriff auf Fachanwendungen der zentralen Telematikinfrastruktur-Plattform wird für Fachmodule des Konnektors auf gesicherte Fachdienste und für Clientsysteme bzw. Fachmodule im LAN des Leistungserbringers auf offene Fachdienste ermöglicht. Die Kommunikation mit aktiven Bestandsnetzen erfolgt ebenfalls nur über den VPN-Tunnel der zentralen Telematikinfrastruktur-Plattform.

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

VPN-Client

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

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

Sicherheitsmodul (gSMC-K) gespeichert ist. Der VPN-Kanal zum VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform (siehe FTP_ITC.1/NK.VPN_TI für die Kommunikation mit der Telematikinfrastruktur) stellt eine Absicherung der Kommunikationsbeziehung zwischen Netzkonnektor und VPN-Konzentrator auf Netzwerkebene dar. Nach erfolgtem Aufbau des VPN-Tunnels zur Telematikinfrastruktur durch den Netzkonnektor (= Teil des EVG) nutzt der Anwendungskonnektor (= IT-Umgebung) diesen Kanal und authentisiert[3] die Organisation des Leistungserbringers gegenüber den Fachdiensten. Dazu nutzt der Anwendungskonnektor Schlüsselmaterial, welches auf einem der Organisation des Leistungserbringers zugeordneten Sicherheitsmodul (SM-B) gespeichert ist.

TLS Kanal[4]

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

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

Die über den TLS-Kanal transportierten Daten werden teilweise auf Anwendungsebene weiter geschützt, beispielsweise durch mit einem HBA erstellte Signaturen.

Zeitdienst

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

DNS-Dienst

Der EVG stellt an der LAN-Schnittstelle die Funktion eines DNS-Servers zur Verfügung.

DHCP-Dienst

Die Sicherheitsfunktion “DHCP-Dienst” ist Bestandteil des Konnektors. Der EVG stellt an der LAN-Schnittstelle die Funktion eines DHCP Servers gemäß RFC 2131 [66] und RFC 2132 [67] zur Verfügung.

---

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

[4] Die Basisdienste zum Aufbau von TLS-Kanälen werden vom Anwendungskonnektor implementiert sind aber formal dem Netzkonnektor zugeordnet.

1.3.1.2. Sicherheitsfunktionen des Anwendungskonnektors (AK)

SCaVA

Der EVG stellt als SCaVA (Signature Creation Application and Signature Validation Application) einen Signaturdienst zur Erstellung und Prüfung von qualifizierten Signaturen nach der eIDAS-VO [12] und nicht qualifizierten Signaturen bereit.

Er führt über die eHealth-Kartenterminals zu signierende Daten den (qualifizierten) Signaturerstellungseinheiten für die Erstellung von (qualifizierten) Einzel- und Stapelsignaturen und Komfortsignaturen über ein lokales Netz zu.

Der Signaturdienst ist für die Erstellung einer begrenzten Anzahl von qualifizierten Signaturen nach der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der qualifizierten Signaturerstellungs¬einheit (QSEE) mit entfernter und lokaler PIN-Eingabe geeignet (Stapelsignatur nach [21]). Der Signaturdienst unterstützt darüber hinaus die Erstellung von qualifizierten Einfachsignaturen (s.a. [21]) mit lokaler und entfernter PIN-Eingabe.

Der Signaturdienst ist für die Erstellung qualifizierter elektronischer Signaturen durch mehrere Benutzer in einem lokalen Netz vorgesehen, d. h. jeder Signaturschlüssel-Inhaber nutzt zur Erstellung dieser Signaturen die Benutzerschnittstelle zum Clientsystem von jedem konfigurierten Arbeitsplatz des lokalen Netzes und seine an einem vor physischen Zugriff geschützten Bereich befindlichen QSEE, dem Heilberufsausweis (HBA).

Bei Aktivierung der Komfortsignatur authentisiert sich der Karteninhaber jeweils für eine HBA- Kartensitzung einmalig mittels Signatur-PIN und es wird, falls noch nicht vorhanden, ein Secure Messaging Kanal zwischen Konnektor und Signaturkarte aufgebaut. Der Authentisierungzustand für die HBA-Kartensitzung (CardSession) wird solange aufrecht erhalten bis ein der HBA-Kartensitzung zugeordneter Zähler für Signaturen oder ein Timer abgelaufen sind. Die Maximalwerte für Signaturzähler und Timer können global für alle HBA-Kartensitzungen konfiguriert werden.

Der Signaturdienst kann für die Erstellung digitaler (nicht-qualifizierter) Signaturen mit anderen Chipkarten und für die Prüfung digitaler (nicht-qualifizierter) Signaturen verwendet werden.

Kryptomodul

Der EVG stellt als Kryptomodul einen Verschlüsselungsdienst zur Verschlüsselung und Entschlüsselung von Dokumenten bereit, die von Clientsystemen, dem VSDM Fachmodul oder anderen Fachmodulen übergeben und nach der Bearbeitung an diese zurückgegeben werden. Der Verschlüsselungsdienst benutzt den Zertifikatsdienst und eine lokale oder entfernte Eingabe der Kartenhalter-PIN für den Zugriff auf die kryptographischen Schlüssel der Chipkarten. Er steht den Clientsystemen zur Benutzung zur Verfügung.

Der EVG stellt als Kryptomodul eine gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und Fachdiensten bereit. Die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem über das lokale Netz der

Leistungserbringer (LE-LAN) ist konfigurierbar, d.h. wenn sie eingerichtet ist, wird sie durch den EVG erzwungen, und entfällt, sofern sie nicht eingerichtet wurde. Die gesicherte Kommunikation zwischen Fachmodulen und Fachdiensten wird auf Anforderung der Fachmodule hergestellt.

Server für Sicherheitsdienste

Der EVG stellt den Kartenterminaldienst zur Nutzung der eHealth-Kartenterminals und den Chipkartendienst zur Nutzung der Chipkarten in den eHealth-Kartenterminals gemäß Spezifikation Konnektor [27] zur Verfügung und erbringt Sicherheitsfunktionalität für deren sichere Nutzung und den Schutz der Ressourcen.

Der EVG kommuniziert mit den eHealth-Kartenterminals (eHKT, s. [38]) im LE-LAN über gesicherte Verbindungen. Diese Verbindungen beruhen auf dem Einrichten der eHealth-Kartenterminals im LE-LAN (einschließlich Pairing), der gegenseitigen Authentisierung des EVG und der eHealth-Kartenterminals und der Sicherung der Vertraulichkeit und der Integrität der übertragenen Daten durch TLS-Kanäle.

Der EVG stellt den Chipkartendienst für den Zugriff auf in eHealth-Kartenterminals gesteckte Karten, die lokale und entfernte PIN-Eingabe und die Card-to-Card-Authentisierung als gekapselte Funktionalität zur Verfügung und nutzt sie selbst im Rahmen anderer Sicherheitsdienste. Der EVG kontrolliert den Zugriff auf Chipkarten in Abhängigkeit von deren Sicherheitszustand.

Fachmodul „Versichertenstammdatenmanagement“

Der EVG umfasst das Fachmodul VSDM. Es unterstützt die Anwendungsfälle der Fachanwendung VSDM, indem es dem Clientsystem anwendungsspezifische Schnittstellen zum Auslesen der Versichertenstammdaten der eGK und der KVK anbietet. Dazu nutzt es Funktionalitäten, die der Anwendungskonnektor anbietet, wie z.B. Zugriff auf die Karten. Um die Aktualität der VSD auf der eGK zu prüfen, kommuniziert das Fachmodul unter Nutzung des fachanwendungsspezifischen Intermediärs VSDM mit dem Fachdienst des Kostenträges des Versicherten und aktualisiert bei Bedarf die VSD.

Das Fachmodul ist verantwortlich für die fachlichen Abläufe der Fachanwendung VSDM im Konnektor. Wesentliche Teile des Funktionsumfangs sind: Lesen der Versichertendaten von der eGK bzw. von der KVK, Prüfen der Vorbedingungen, Kommunikation mit den Fachdiensten, um die eGK zu aktualisieren und Erstellung des Prüfungsnachweises [37].

Anwendungshinweis 1: Der Begriff VSDM Fachdienst umfasst im Rahmen dieses Security Targets auch den Intermediär VSDM. Dieses bedeutet, dass bei einer Beschreibung einer Kommunikation des EVG mit dem VSDM Fachdienst stets die Tatsache berücksichtigt wurde, dass der EVG nur mit dem Intermediär VSDM kommuniziert und nicht direkt mit dem Fachdienst VSDM

Unterstützung des zentralen Verzeichnisdienstes

Der Konnektor besitzt einen LDAP-Proxy und unterstützt die Nutzung des zentralen Verzeichnisdienstes der TI.

Sichere Kommunikation zur ePA Fachanwendung

Der EVG bietet einen sicheren Kanal zur Dokumentenverwaltung des ePA-Aktensystems (VAU-Kanal) und sichere Kommunikation zur Schlüsselableitungen mit den Schlüsselgenerierungsdiensten (SGD-Protokoll) an.

1.3.2. Einsatzumgebung des Konnektors

Der EVG besteht aus einem selbständigen Gerät (Konnektorgerät) und wird in der Einsatzumgebung der Leistungserbringer (LE) verwendet. Das Konnektorgerät wird im Betrieb vor physischen Zugriff geschützt (siehe auch A.NK.phys_Schutz bzw. A.AK.phys_Schutz). Die Betriebsumgebung des EVG ist ein geschützter Einsatzbereich.

Die Einsatzumgebung des Konnektors als Einbox-Lösung ist in der folgenden Abbildung 2 dargestellt. Insbesondere wird der Konnektor immer mit einer gSMC-K gemeinsam betrieben, wobei die gSMC-K durch die gematik zugelassen wurde.

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

- Netzkonnektor und Anwendungskonnektor in einer Box integriert sind, und dass
- die gSMC-K sicher mit dem Konnektor verbunden ist, so dass kein weiterer Schutz der Verbindung zwischen Konnektor und gSMC-K erforderlich wird. Der physische Zugriff auf die benannten Schnittstellen ist durch A.NK.phys_Schutz bzw. A.AK.phys_Schutz ausgeschlossen. Der logische Schutz der Schnittstellen ist Teil der Sicherheitsfunktionalität, die Gegenstand des EVG ist.

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

Alle Teilkomponenten des Konnektors sind durch dicke schwarze Rahmen gekennzeichnet. Der Netzkonnektor und Anwendungskonnektor inkl. VSDM-Fachmodul (Teile des EVG) sind durch dunkelblaue Färbung kenntlich gemacht. Die gSMC-K als fester Bestandteil des Konnktors (nicht Teil des EVG) ist hellblau dargestellt. Durch die dunkelblaue Färbung wird die physische EVG-Abgrenzung des Konnektors beschrieben. Mit der roten Linie werden zum besseren Verständnis Komponenten zusammengefasst, die in einem gemeinsamen Gehäuse untergebracht sind oder die üblicherweise auf einer gemeinsamen Plattform ablaufen. Die rote Linien beschreibt den physikalisch geschützten Bereich (vgl. A.NK.phys_Schutz bzw. A.AK.phys_Schutz).

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

Anwendungshinweis 2: Die Bereiche, die durch die Einsatzumgebung zu schützen sind werden in Abbildung 2 als rote Box dargestellt.

In der folgenden Abbildung 2 bedeuten die Abkürzungen (siehe auch Kapitel 7.1 in [16]):

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

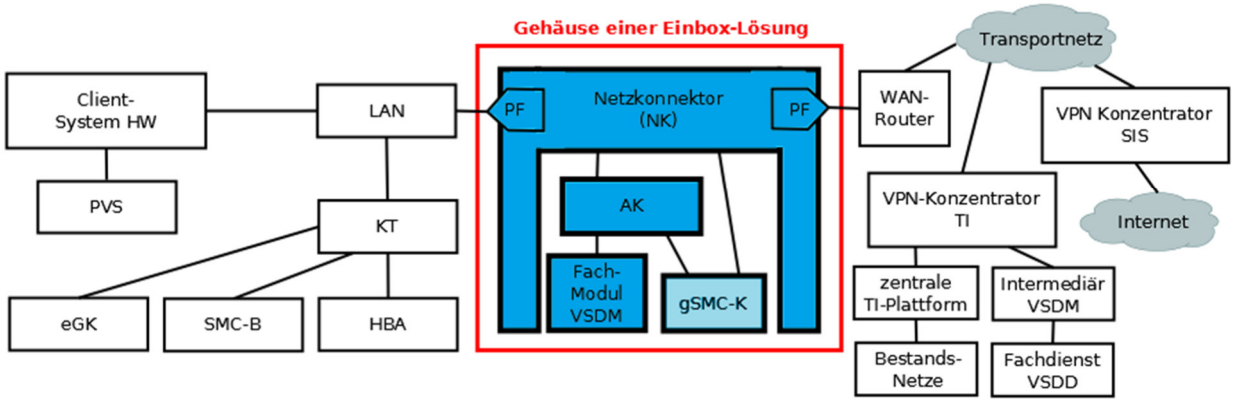

Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung)

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

Bei der hier als Einbox-Lösung bezeichneten Variante handelt es sich um eine typische Lösung für kleinere und mittlere Arztpraxen oder Apotheken: Netzkonnektor und Anwendungskonnektor laufen in einer gemeinsamen Box ab.

Es wird angenommen, dass die Einsatzumgebung des Konnektors diesen vor physischen Angriffen schützt (siehe Annahme A.NK.phys_Schutz bzw. A.AK.phys_Schutz).

Es wird angenommen, dass die Clientsysteme nicht oder nur in sicherer Weise an potentiell unsichere Netze (z. B. Internet) angebunden sind. Ferner wird angenommen, dass die Clientsysteme nach dem aktuellen Stand der Technik entwickelt wurden und administriert werden, so dass sie das spezifizierte Verhalten zeigen. Für Details siehe zum Beispiel Annahme A.NK.Betrieb_CS in Abschnitt 3.4.

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 3: Der EVG unterstützt alle vom PP [16] erwarteten physischen Schnittstellen und implementiert darüber hinaus herstellerspezifische Schnittstellen wie im Folgenden dargestellt.

Der EVG besitzt folgende physische Schnittstellen:

PS1 Entfällt aufgrund der Einbox-Lösung.

Anmerkung 1. In diesem ST wird die Nummerierung aus dem NK-PP [17] übernommen. Durch die für dieses ST relevante Einboxlösung des Konnektors ist die Identifizierung einer physischen Schnittstelle zwischen Netzkonnektor und dem Anwendungskonnektor nicht relevant. Die Kommunikation beider Konnektorteile beschränkt sich auf die logische Schnittstelle LS1.

PS2 Eine Schnittstelle zum LAN bzw. zum Clientsystem.

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

PS3 Eine Schnittstelle zu Datennetzen (WAN), welche als Transportnetz für den Zugang zur Telematikinfrastruktur und SIS dienen. Es wird angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und Verbindungen mit ihnen nicht notwendigerweise verschlüsselt sind. Da der EVG zwei Netzwerkkarten nutzt, findet eine physische Trennung des LAN- bzw. WAN-Zugangs über die Netzwerkkarten statt. Die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle fallen nicht in einer physischen Schnittstelle zusammen.

Anwendungshinweis 4: Die mit PS2 bezeichnete LAN-Schnittstelle und die mit PS3 bezeichnete WAN-Schnittstelle sind durch separate Netzwerkcontroller physisch getrennt.

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

Die gSMC-K dient als sicherer Schlüsselspeicher für die **kryptographische Identität** des EVGs in Form privater Authentisierungsschlüssel und der zugehörigen Zertifikate.

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

PS5 Schnittstelle zu einer Signaleinrichtung mit Status LEDs

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

PS6 Eine USB Schnittstelle.

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

PS7 Eine Schnittstelle für den Werksreset.

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

Schließlich wird die physische Hülle des Konnektors als weitere Schnittstelle betrachtet. Aufgrund der Annahme A.NK.phys_Schutz bzw. A.AK.phys_Schutz werden keine Angriffe über diese Schnittstelle betrachtet. Die Abbildung 3 zeigt die verfügbaren physischen Schnittstellen des Konnektors sowie deren Zuordnung zu den logischen Schnittstellen. Der Stromanschluss ist keine relevante Schnittstelle im Sinne des zugrundeliegenden PP [16].

Anwendungshinweis 5: Die Schnittstellen sind in Abbildung 2 und Abbildung 3 grafisch dargestellt.

1.3.3.2. Logische Schnittstellen des EVG

Anwendungshinweis 6: Der folgende Abschnitt stellt eine Übersicht über die logischen Schnittstellen des EVG samt ihrer Zuordnung zu den in Kapitel 1.3.3.1 beschriebenen physischen Schnittstellen dar. Alle logischen Schnittstellen aus dem PP [16] sind enthalten. Es sind zusätzliche Schnittstellen definiert worden.

Der EVG besitzt folgende logische Schnittstellen:

LS1 (gelöscht)

Anmerkung 2. Die logische Schnittstelle LS1 stellt in Anlehnung an das NK-PP [17] eine Schnittstelle zwischen Netzkonnektor und Anwendungskonnektor dar. Nach PP [16] ist dies für den EVG keine externe Schnittsteller mehr und wurde daher entfernt.

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

LS3 Eine Schnittstelle zu den Fachmodulen, die im Konnektor laufen. Da die Kommunikation innerhalb des Konnektors erfolgt, wird hier keine physische Schnittstelle zugeordnet.

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

LS5 Eine Schnittstelle zum SIS, die mittels eines Virtual Private Networks (VPN) über das Transportnetz (WAN, via PS3) erreicht wird.

LS6 Eine Schnittstelle zu Fachdiensten, die mittels eines VPN über das Transportnetz (WAN, via PS3) erreicht werden.

LS7 Eine Schnittstelle zu PKI- und anderen Diensten (WAN, via PS3). Dazu zählen der TSL-Dienst, der CRL-Download, sowie OCSP-Dienst.

LS8 Eine Schnittstelle zum Konfigurationsdienst KSR (WAN, via PS3).

LS9 Eine Schnittstelle zu eHealth-Kartenterminals (LAN, via PS2).

LS10 Eine Schnittstelle zu Chipkarten außerhalb des EVG, die über eHealth-Kartenterminals angesprochen werden (LAN, via PS2).

LS11 Eine Schnittstelle zu lokalen Managementfunktionen (Software/Firmware, TSL-Updates, Firewall-Konfiguration) des Konnektors (via PS2).

LS12 Eine Schnittstelle zu einem Sicherheitsmodul für den Konnektor (gSMC-K) (via PS4).

LS13 Eine Schnittstelle zu entfernten Managementfunktionen für den Konnektor gemäß Konnektor-Spezifikation [27], Abschnitt 4.3.8 (via PS2).

LS14 Eine Schnittstelle zur Signaleinrichtung zur Anzeige von Hinweisen an den Administrator über kritische Betriebszustände des Konnektors gemäß Konnektor-Spezifikation [27], Abschnitt 3.3 (via PS5).

LS15 Eine USB-Schnittstelle (via PS6) zur initialisierung des EVG. Im Operativen Betrieb wird diese Schnittstelle nicht verwendet und daher nicht weiter betrachtet. Insbesondere werden keine Bedrohungen in Bezug auf diese Schnittstelle betrachtet, da die Schnittstelle aufgrund der Annahmen an die Zugänglichkeit als sicher zu betrachten ist (siehe A.NK.phys_Schutz bzw. A.AK.phys_Schutz sowie A.NK.Admin_EVG)

LS16 Eine Schnittstelle zum Auslösen des Werksreset (via PS7). Im Folgenden werden keine Bedrohungen in Bezug auf diese Schnittstelle betrachtet, da die Schnittstelle aufgrund der Annahmen an die Zugänglichkeit als sicher zu betrachten ist (siehe A.NK.phys_Schutz bzw. A.AK.phys_Schutz sowie A.NK.Admin_EVG)

LS17 Eine Schnittstelle zur Vertrauenswürdige Ausführungsumgebung (VAU) der Fachanwendung ePA

LS18 Eine Schnittstelle zu den Schlüsselgenerierungsdiensten SGD1 und SGD2 für die Nutzung der Fachanwendung ePA.

Das lokale und entfernte Management des Netzkonnektors erfolgt über die LAN- Schnittstelle die vom Netzkonnktor bereitgestellt werden.

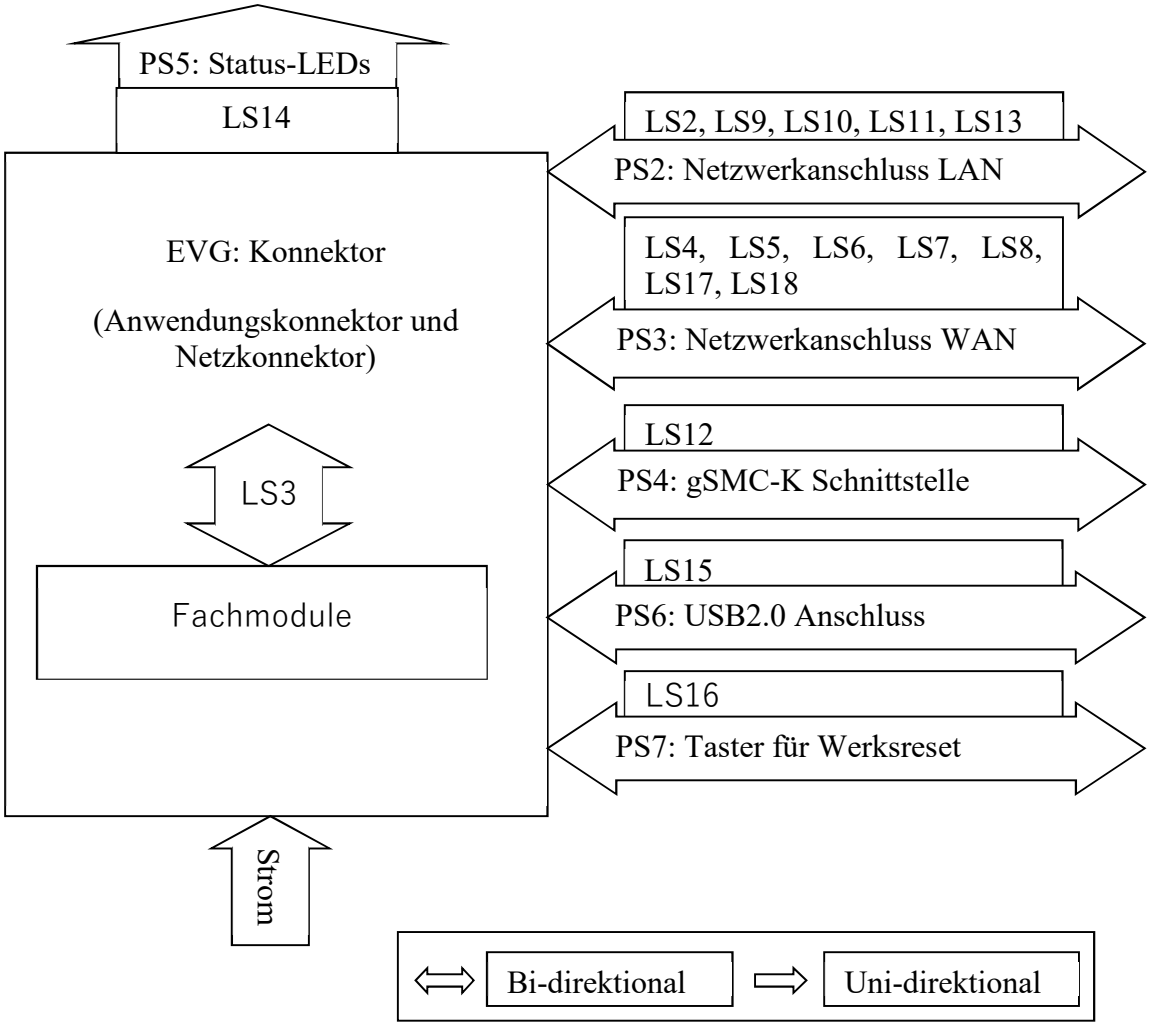

Abbildung 3: Konnektor: externe, physische und logische Schnittstellen

1.3.4. Aufbau und physische Abgrenzung des Konnektors

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

Anwendungshinweis 7: Die Abbildung 4, Abbildung 5, Abbildung 6 und Abbildung 7 stellen das allgemeine Architekturkonzept des Konnektors dar (EVG).

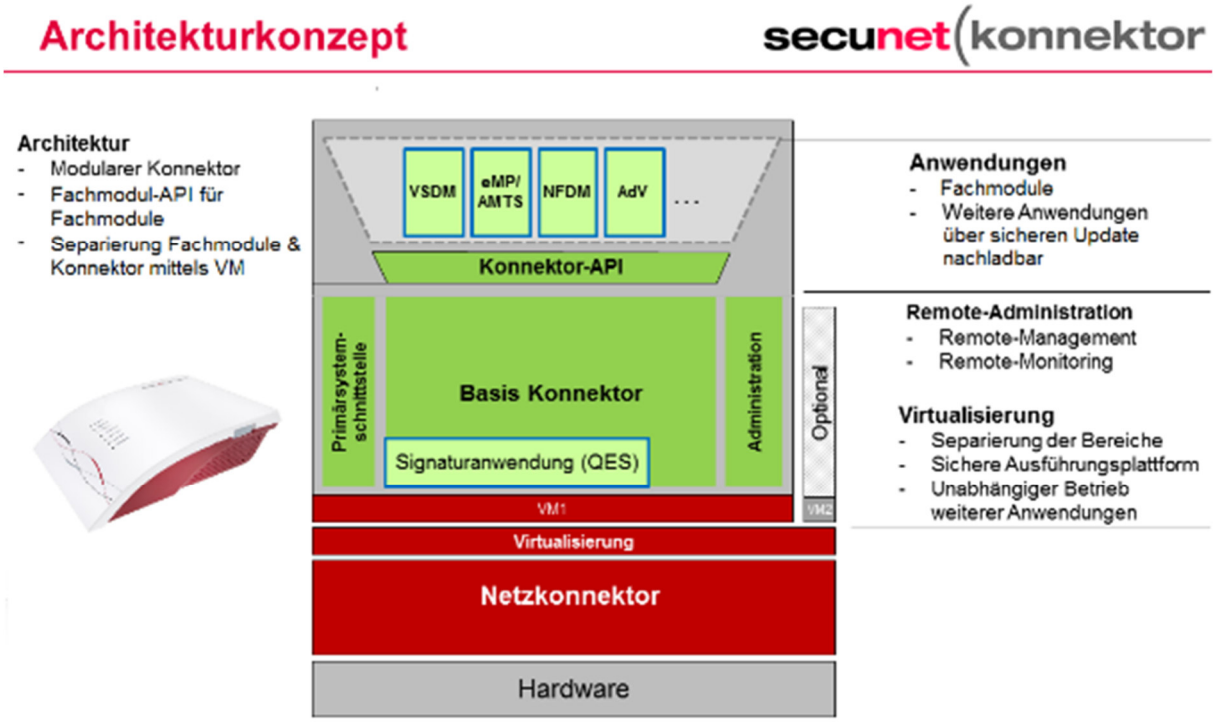

Abbildung 4: Konnektor Architekturkonzept (schematisch)

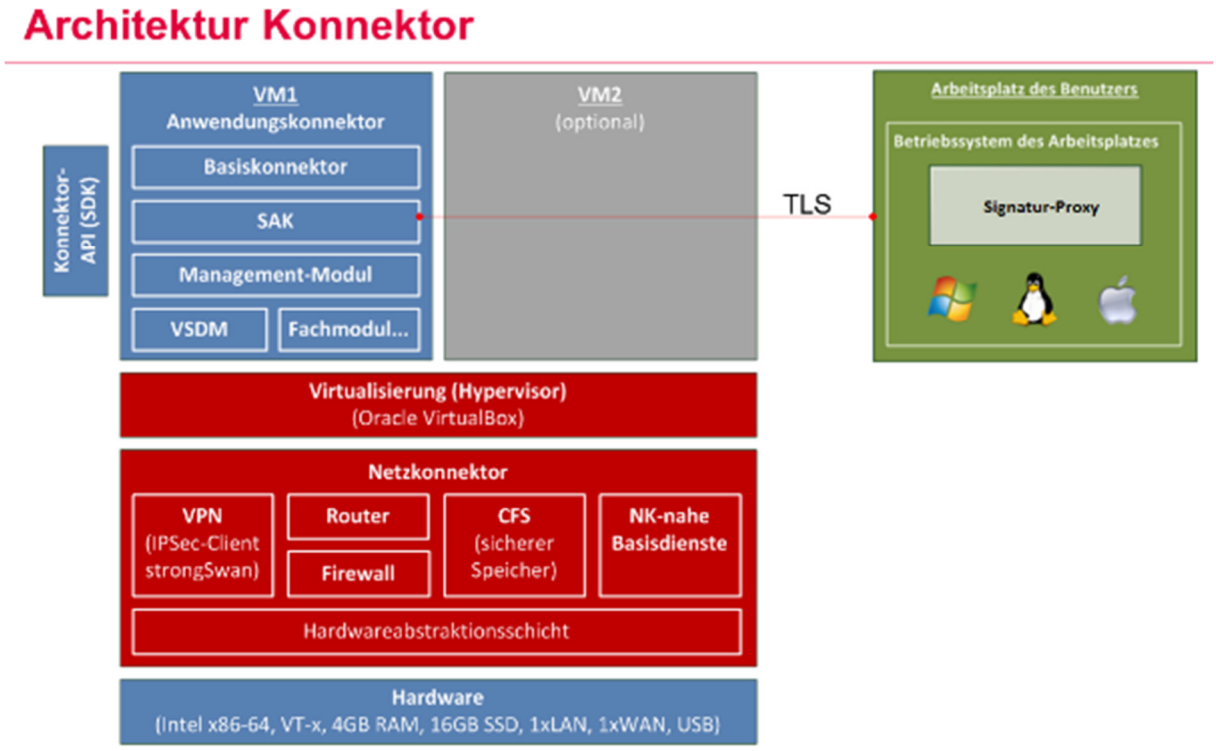

Abbildung 5: Konnektor Architektur Komponentenansicht (schematisch)

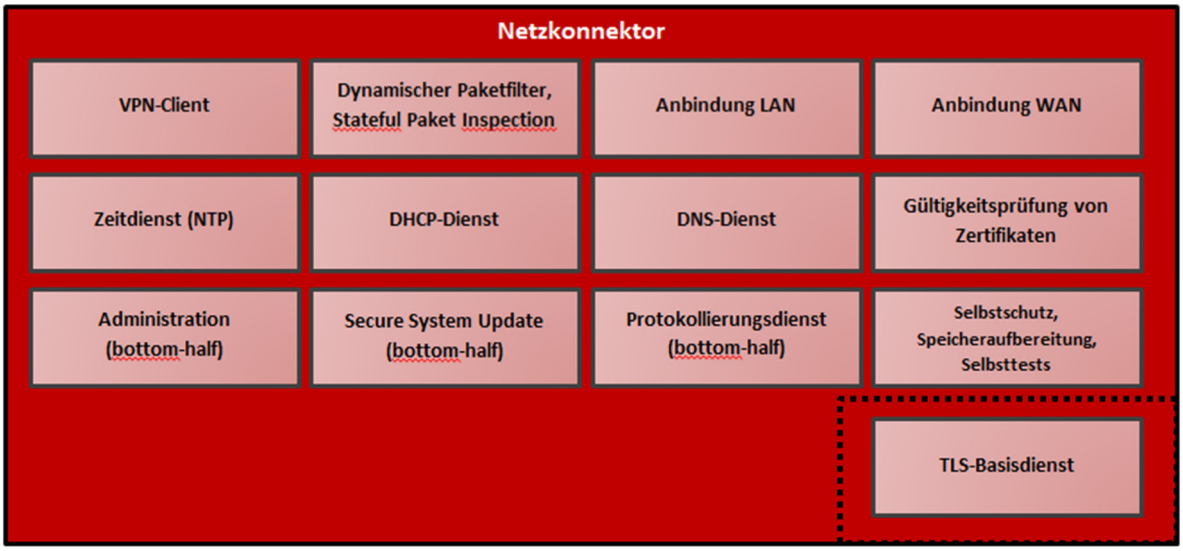

Abbildung 6: Netzkonnektor Komponenten (Der TLS-Basisdienst wird im Anwendungskonnektor umgesetzt, ist aber formal dem Netzkonnektor zugeordnet)

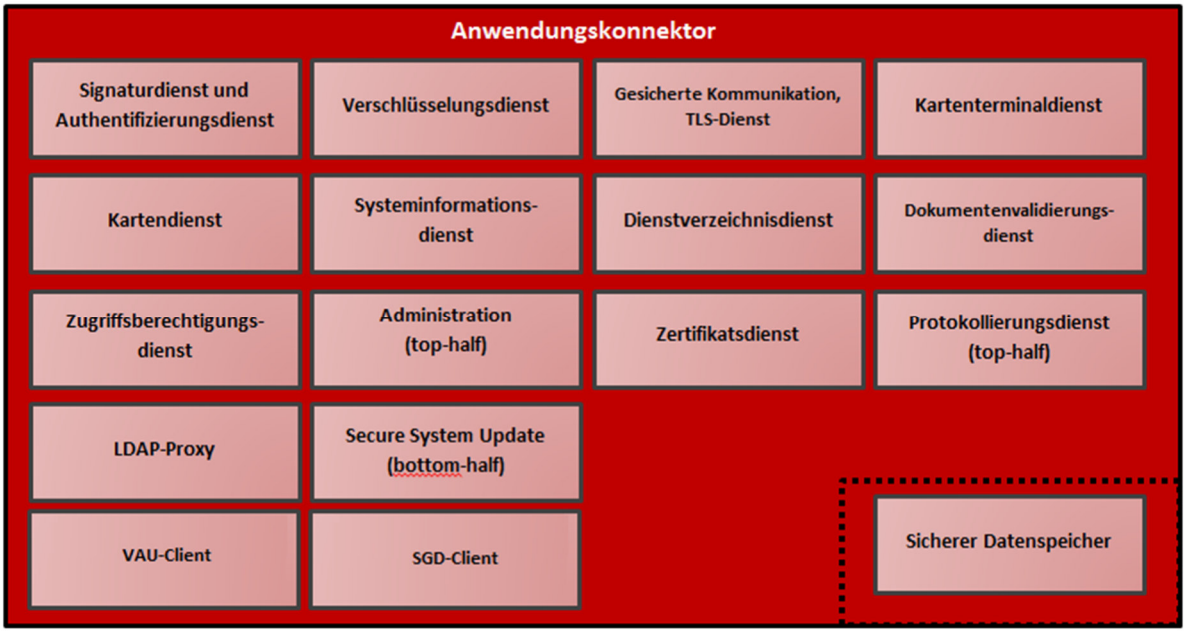

Abbildung 7: Anwendungskonnektor Komponenten (Der Sichere Datenspeicher wird im Netzkonnektor umgesetzt, ist aber formal dem Anwendungskonnektor zugeordnet)

Architekturübersicht

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

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

- Die virtuelle Maschine VM1 enthält den Anwendungskonnektor, der aus Basiskonnektor, Management-Modul und den Fachmodulen besteht. Weiterhin ist der Signaturdienst in dieser VM beheimatet. Der Fachmodulkonnektor ergibt sich aus den für Fachmodule vorgesehenen Schnittstellen des Basiskonnektors und des Netzkonnektors. Als Betriebssystem in VM1 kommt ein minimalisiertes Linux zum

Einsatz. Die beschriebene Funktionalität bildet den EVG. Die virtuelle Maschine VM2 ist optional und für Erweiterungen vorgesehen.

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

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

1.3.5. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste

Der EVG bestehend aus den Komponeneten Netzkonnektor und Anwendungskonnektor erbringt die im Folgenden beschriebene Sicherheitsfunktionalität.

1.3.5.1. Vom Netzkonnektor erbrachte Sicherheitsdienste

Der EVG erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [27] definierten Schnittstellen weitgehend automatisch. Die Abbildung 6 zeigt die architektonische Aufteilung der im Folgenden beschreibenden Sicherheitsdienste des Netzkonnektors.

Anwendungshinweis 8: **Authentisierung des Administrators**: Der EVG sieht einen gemeinsamen Administrator-Account für NK und AK vor. Die Authentisierung des Konnektor-Administrators wird vom Managementmodul des AKs vorgenommen. Der AK setzt nach erfolgreicher Authentisierung den Authentisierungszustand und autorisert auf diese Weise die Zugriffe des Administrators. Es wird keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) durchgeführt. Der Authentisierungszustand ist Aufgrund der Annahme A.NK.phys_Schutz vor Manipulation abgesichert.

Anwendungshinweis 9: **Vollständigkeit der Dienste:** Die Dienste des EVGs wurden aus [16] bzw. aus dem NK-PP [17] übernommen und entsprechend der dort verankerten Freiheitsgrade präzisiert.

Anwendungshinweis 10: **Transaktionssicherheit:** Der Netzkonnektor gewährleistet keine Transaktionssicherheit. Soweit Transaktionssicherheit aus Sicherheitsgründen erforderlich ist, wird sie im Clientsystem und/oder in der zentralen Telematikinfrastruktur-Plattform hergestellt.

Der EVG erbringt gemäß [16] bzw. NK-PP [17] folgende Sicherheitsdienste:

VPN-Client:

Der EVG stellt einen sicheren Kanal (virtual private network, VPN) zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) zwecks Nutzung von Diensten bereit. Der

sichere Kanal zur TI wird zur Kommunikation zwischen Anwendungskonnektor und Fachdiensten, Netzkonnektor und zentralen Diensten sowie zwischen Clientsystemen und Bestandsnetzen genutzt. Ferner stellt der EVG einen sicheren Kanal (VPN) zum SIS her. Dieser Kanal dient der Verbindung der lokalen Netzwerke der Leistungserbringer mit dem Internet.

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

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

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

Der Netzkonnektor erzwingt die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen und verbietet ungeschützten Zugriff auf das Transportnetz. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[5], aber er muss ihre versehentliche Preisgabe verhindern.

Dynamischer Paketfilter:

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

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

Verbindungsaufbau erforderlichen Kommunikation[6] sowie Verbindungen zum CRL Download Server.

Anwendungshinweis 11: Der **LAN-seitiger Paketfilter** hindert Schadsoftware, die möglicherweise auf anderen Wegen (z. B. Wechseldatenträger wie CD, DVD, USB-Stick, Diskette) in die IT-Systeme im LAN des Leistungserbringers kommt daran, die Integrität des Konnektors zu bedrohen.

Anwendungshinweis 12: Der Netzkonnektor enthält kein **Application Layer Gateway**. Der Anwendungskonnektor wird topologisch von beiden Seiten von einem Paketfilter umgeben (LAN-seitig und WAN-seitig, d.h. gegenüber dem Clientsystemnetz und gegenüber dem Transportnetz; siehe auch Abbildung 2).

TLS-Basisdienst:

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

Anwendungshinweis 13: Hinweis: Die Entscheidung, für welche Verbindungen diese TLS-Kanäle genutzt werden, liegt beim Anwendungskonnektor. Der TLS-Basisdienst wird durch den Netzkonnektor umgesetzt. Formal ist diese Komponente dem Anwendungskonnektor zugeordnet.

Der EVG bietet folgende netzbasierte Dienste an:

Zeitdienst:

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

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

Anwendungshinweis 14: Der EVG implementiert eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK (Siehe auch Konnektor-Spezifikation [27], Anforderung 352 TIP 1 A 4788). Die Zeitsynchronisation erfolgt ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform, d.h. über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur.

DHCP-Dienst:

Der EVG stellt an der LAN-Schnittstelle (PS2) die Funktion eines DHCP Servers gemäß RFC 2131 [66] und RFC 2132 [67] zur Verfügung.

DNS-Dienst:

Der EVG stellt an der LAN-Schnittstelle (PS2) und an der Schnittstelle zum Anwendungskonnektor (LS1) die Funktion eines DNS-Servers zur Verfügung.

Gültigkeitsprüfung von Zertifikaten:

Der EVG überprüft die Gültigkeit der Zertifikate des Kommunikationspartners, die für den Aufbau eines VPN-Kanals verwendet werden.[7] Zu diesem Zweck wird eine TSL (Trust-Service Status List) verteilt, welche Zertifikate von Diensteanbietern enthält, die Gerätezertifikate ausstellen können. Der EVG kann anhand der aktuell gültigen TSL die Gültigkeit der Gerätezertifikate seiner Kommunikationspartner prüfen. Ferner wird eine zugehörige CRL (Certificate Revocation List) bereitgestellt, die der EVG ebenfalls auswertet. Außerdem überprüft der EVG, dass die verwendeten Algorithmen gültig sind. Siehe auch Sicherheitsdienst VPN-Client (a): Authentisierung der Kommunikationspartner).

Anwendungshinweis 15: Der EVG führt keine explizite Prüfung der Algorithmen auf deren Gültigkeit gegenüber den Vorgaben in TR-03116-1[19] durch. Die Verwendung von gültigen Algorithmen wird durch das Aufbringen eines korrekten und evaluierten Softwarestandes des EVG unter Nutzung des sicheren Updatemechanismus sichergestellt.

Stateful Packet Inspection:

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

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

Anwendungshinweis 16: Der Konnektor realisiert kein netzwerkbasiertes Intrusion Detection System (IDS) für das Clientsystemnetz.

Darüber hinaus implementiert der EVG folgende übergeordnete Dienste:

Selbstschutz:

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

Speicheraufbereitung:

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

Selbsttests:

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

Protokollierung:

Der EVG führt ein Sicherheits-Log (security log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher ist hinreichend groß dimensioniert. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [27].

Anwendungshinweis 17: Eine (über die Anforderungen der Konnektorspezifikation [27] hinausgehende) Auswertung des Sicherheits-Logs durch den Netzkonnektor erfolgt nicht.

Anwendungshinweis 18: Die geschützte Speicherung des Protokolls (u. a. zyklisches Überschreiben, Schutz gegen Manipulation durch den Administrator) wird im PP [16] als übergreifende Funktionalität von NK und AK gefordert (siehe auch FAU_STG.1/AK und FAU_STG.4/AK).

Administration:

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

Der EVG bietet eine lokale und entfernte Managementschnittstelle an.

Anwendungshinweis 19: Der EVG bietet die Möglichkeit eines sicheren SW/FW/Konfigurations- und TSL-Updates über die Managementsschnittstellen an. Weitere Managementfunktionen werden gemäß FMT_MTD.1.1/NK umgesetzt.

Eine Möglichkeit zur Fernwartung ist gemäß Konnektor-Spezifikation [27], Abschnitt 4.3 implementiert. Zur Absicherung der Fernwartung werden dieselben Mechanismen verwendet wie zur Absicherung der lokalen Administration an der LAN-Schnittstelle (sicherer Kanal zwischen Administrator-Arbeitsplatz und Netzkonnektor siehe FTP_TRP.1/NK.Admin, Autorisierung des Administrators siehe FIA_UAU.1/NK.SMR). Es ist jedoch zu beachten, dass laut Konnektorspezifikation (Kapitel 4.3.8) bei einer Managementverbindung über die WAN Schnittstelle der Verbindungsaufbau immer vom Konnektor ausgeht.

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

Secure System Update:

Der EVG ermöglicht das sichere Einspielen von Softwareupdates und stellt dabei die Authentizität und Integrität der Update-Daten sicher. Dabei können die Softwareanteile des Netzkonnektors und des Anwendungskonnektors aktualisiert werden.

1.3.5.2. Vom Anwendungskonnektor erbrachte Sicherheitsdienste

Über die im vorigen Abschnitt 1.3.5.1 genannten Dienste hinaus bietet der EVG-Teil Anwendungskonnektor folgende Sicherheitsdienste an:

Signaturdienst:

Der EVG ermöglicht im Sinne der eIDAS-VO [12] die Erstellung und Prüfung qualifizierter elektronischer Signaturen (QES). Zudem wird die Erstellung und Prüfung von nichtqualifizierten elektronischen Signaturen (nonQES) ermöglicht. Bei der Signaturerstellung sind sowohl Einzelsignaturen als auch Stapelsignaturen und Komfortsignaturen möglich. Als qualifizierte Signaturerstellungseinheit (QSEE) kommt für QES ein Heilberufsausweis (HBA) mit QES-Signaturschlüsseln zum Einsatz. Für die Erzeugung der nonQES-Signatur wird ein HBA oder die SM-B[8] mit non-QES-Signaturschlüsseln verwendet.

[8] SM-B schließt SMC-B und HSM-B ein.

Für die Beschreibungen in dem vorliegenden Schutzprofil wird der Begriff der **Signaturrichtlinie** benutzt. Eine Signaturrichtlinie ist ein Satz von Regeln, wie die Daten zu signieren bzw. zu prüfen sind, und umfasst alle Parameter, die für die Signaturerstellung, bzw. Signaturprüfung der signierten Daten nach dem identifizierten Standard notwendig sind.

Eine genauere Beschreibung des Begriffes Signaturichtlinie findet sich in [16], Kapitel 1.3.5.2. Dort findet sich auch ein beispielhafter Ablauf einer qualifizierten Signatur-Erzeugung sowie einer qualifizierten Signatur-Prüfung im Fall der fehlerfreien Ausführung.

Anwendungshinweis 20: Die genauen Abläufe sind der Spezifikation Konnektor [27] und den dort referenzierten Dokumenten zu entnehmen.

Anwendungshinweis 21: S.o.

Verschlüsselungsdienst:

Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an. Im Fall der hybriden Verschlüsselung kann die (asymmetrische) Verschlüsselung für mehrere Identitäten, repräsentiert durch X.509 Zertifikate oder durch öffentliche Schlüssel, erfolgen. Zertifikate werden vor Verwendung auf ihre Gültigkeit geprüft. Bei hybrider Entschlüsselung erfolgt die asymmetrische Entschlüsselung in der entsprechenden Chipkarte. Laut Spezifikation Konnektor [27] werden dazu die Module SM-B, eGK und HBAx unterstützt.

Als Bestandteil des Verschlüsselungsdienstes müssen symmetrische Schlüssel erzeugt werden können. Dazu erfüllt der EVG die Anforderungen von TR-03116-1 [19] zur Erzeugung von Zufallszahlen.

Der Verschlüsselungsdienst bietet für alle unterstützten Dokumentenformate die hybride und symmetrische Ver- und Entschlüsselung nach dem Cryptographic Message Syntax Standard (CMS, RFC 5652, [78]) an. Darüber hinaus wird die formaterhaltende hybride Ver-/Entschlüsselung von XML Dokumenten nach [79] unterstützt.

Für die verwendeten Algorithmen und deren Konfiguration werden bestehende Standards eingehalten, um eine Interoperabilität zwischen verschiedenen Herstellerimplementierungen zu erreichen.

Sicherer Datenspeicher:

Der sichere Datenspeicher bildet einen internen Dienst des Konnektors für die dauerhafte Speicherung aller sicherheitskritischen, veränderlichen Benutzerdaten und TSF-Daten, die für seinen Betrieb relevant sind. Ferner stellt der Konnektor den in ihm laufenden Fachmodulen die Nutzung dieses Datenspeichers für deren sensible Daten zur Verfügung.

Der sichere Datenspeicher sichert die Integrität, Authentizität und die Vertraulichkeit der in ihm hinterlegten Daten im abgeschalteten Zustand des Konnektors. Nur der Konnektor hat auf diesen Datenspeicher Zugriff. Folgende Daten werden im sichern Datenspeicher abgelegt:

- die Konfigurationsdaten des Konnektormanagements,

- die Trust Service List,
- Konfigurationsdaten der eHealth-Kartenterminals, insbesondere deren Administratorpasswörter,
- Daten des Zertifikatsdienstes, insbesondere die Certificate Revocation Lists,
- sonstige Konfigurationsdaten des Konnektors.

Anmerkung 3. Datenobjekte des SDS mit dem Sicherherheitsattribut „Adminstratorobjekt“ werden vom Konnektor nicht unterstützt. Der Sichere Datenspeicher wird durch das CFS des Netzkonnektors umgesetzt. Formal ist diese Komponente dem Anwendungskonnektor zugeordnet.

Gesicherte Kommunikation:

Die Absicherung der Kommunikation über die externen Netzwerk-Schnittstellen erfolgt auf niedriger Netzwerk-Schicht (Layer 3: IPsec) oder über Transport Layer Security (TLS) hinsichtlich Vertraulichkeit, Integrität und Authentizität. Folgende Verbindungen müssen durch TLS abgesichert werden:

- Verbindungen zwischen dem EVG und Clientsystemen zur Nutzung von Fachanwendungen (in Form von Fachmodulen) oder von Basisdiensten des Konnektors[9]. Der Zugriff von Clientsystemen ist durch die Verwendung von Whitelisting einschränkbar;
- Verbindungen zwischen dem EVG und Fachdiensten bzw. deren vorgelagerten Intermediären;
- Verbindungen zwischen dem EVG und eHealth-Kartenterminals;
- Verbindungen zwischen dem EVG und einem externen Managementsystem;
- Verbindungen zwischen dem EVG und dem Konfigurationsdienst.
- Verbindungen zwischen dem EVG und dem TSL-Dienst für den Download der BNetzA-VL und deren Hash-Wert.

Dazu unterstützt der EVG die Erzeugung und den Export von X.509 Zertifikaten und der zugehörigen privaten Schlüssel sowie den Import von X.509 Zertifikaten

TLS Dienst:

[9] Abhängig von der Konfiguration des Konnektors können auch Verbindungen erlaubt werden, die nicht per TLS gesichert sind.

Basierend auf dem TLS-Basisdienst des Netzkonnektors (s. Abschnitt 1.3.5.1) leistet der Anwendungskonnektor folgende Dienste: Fachmodule auf dem Konnektor müssen gesicherte Verbindungen zu Fachdiensten nutzen können. Dazu dient der EVG als Proxy, der jeweils TLS-Kanäle zwischen Fachmodulen und Fachdiensten bzw. den vorgelagerten Intermediären verwaltet[10]. Beim Aufbau dieser TLS-Kanäle wird die Authentizität der Endpunkte durch Verwendung von Zertifikaten überprüft. Bei der Authentisierung gegenüber Fachdiensten kann der Konnektor die Identität einer SMC-B über einen entsprechenden Kanal nutzen. Bei fehlerhafter Authentisierung wird die Verbindung bzw. der Verbindungsaufbau abgebrochen.

Terminaldienst:

Der Terminaldienst umfasst das Management der im lokalen Netz der Leistungserbringer adressierbaren eHealth-Kartenterminals. Er realisiert die Anmeldung (Pairing) von neu hinzugekommenen bzw. die Abmeldung von entfernten Kartenterminals am Konnektor.

Das Pairing neu hinzugekommener Terminals erfolgt über einen zuvor aufgebauten TLS-Kanal und unter Aufsicht eines Administrators: Bei fehlgeschlagener Prüfung des Terminal-Zertifikates beim Aufbau der TLS-Verbindung erfolgt kein Pairing und das Terminal steht nicht zur Verfügung. Im anderen Fall entscheidet der Administrator anhand des an der Managementschnittstelle angezeigten Fingerabdruckes des Terminal-Zertifikates über die Akzeptanz des Kartenterminals. Im Fall einer Zurückweisung dieses Fingerabdruckes wird das Pairing abgebrochen und das Kartenterminal steht für Dienste des Konnektors nicht zur Verfügung.

Verbindungen zu angebundenen Kartenterminals werden durch einen TLS-Keepalive Mechanismus aufrecht erhalten. Der Terminaldienst stellt Informationen über gesteckte Karten für Basisdienste und Fachmodule bereit. Ferner ermöglicht er Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule. Damit können Meldungen zur Anzeige am Display des Terminals veranlasst werden und es können Eingaben des Benutzers am PIN-Pad von Kartenterminals abgefragt werden. Die Managementfunktion der Terminals durch den EVG umfasst auch die Behandlung konkurrierender Zugriffsversuche auf ein Kartenterminal in der Weise, dass ein Terminal einem Vorgang (Transaktion) des EVG exklusiv zur Verfügung gestellt wird, bis der Vorgang abgeschlossen ist.

[10] Siehe auch Sicherheitsdienst „gesicherte Kommunikation“

Chipkartendienst:

Der Chipkartendienst umfasst das Management aller Chipkarten, die in den vom Konnektor verwalteten eHealth-Kartenterminals gesteckt sind. Damit sind alle gesteckten Karten nicht nur identifizierbar und adressierbar, sie sind auch bezüglich ihrer Art und Funktionalität im Konnektor erfasst. Folgende Karten-Typen werden vom Konnektor unterstützt:

- KVK
- eGK (Generation 1+ und 2)
- HBA (Generation 2) sowie HBA-qSig und ZOD-2.0
- SMC-B (Generation 2)
- gSMC-KT (Generation 2)
- gSMC-K (Generation 2)

Die Managementfunktion der Karten durch den EVG umfasst auch die Behandlung konkurrierender Zugriffsversuche auf eine Chipkarte in der Weise, dass ein Karte für einen Vorgang (Session) des EVG exklusiv zur Verfügung gestellt wird, bis der Vorgang abgeschlossen ist.

Der Konnektor unterstützt das Remote-PIN-Verfahren im Sinne der BSI TR-03114 [21]. Weiterhin wird die PIN-Überprüfung, das Ändern, Entsperren und die PIN-Statusabfrage unterstützt.

Systeminformationsdienst:

Der Systeminformationsdienst stellt Ereignisse interner Ereignisquellen des EVG an Basisdienste, Fachmodule und an die bei ihm registrierten Clientsysteme zur Verfügung. Dies erfolgt entweder durch einen Pull-Mechanismus oder Push-Mechanismus.

Der Pull-Mechanismus des Systeminformationsdienstes erlaubt die Abfrage von Zuständen oder statischen Informationen durch Fachmodule und Clientsysteme. Zu diesen Zuständen bzw. Informationen gehören (siehe [27], Kapitel 4.1.6):

- Auflistung der verfügbaren Kartenterminals
- Auflistung der gesteckten Karten
- Auflistung aller HSMs
- Ressourcen-Informationen zu einer gewählten Ressource

Der Push-Mechanismus des Systeminformationsdienstes stellt Ereignisse interner Ereignisquellen des Konnektors aktiv allen Basisdiensten, Fachmodulen und bei ihm registrierten Clientsystemen zur Verfügung. Diese Zustellung erfolgt unidirektional über eine Netzschnittstelle.

Darüber hinaus werden die folgenden Dienste nach [27] umgesetzt:

Dienstverzeichnisdienst:

Der Dienstverzeichnisdienst liefert dem aufrufenden Clientsystem sowohl Informationen über die Version und Produktkenndaten des Konnektors, als auch die SOAP-Endpunkte, über die das Clientsystem die einzelnen Dienstoperationen erreichen kann.

Dokumentenvalidierungsdienst:

Der Dokumentenvalidierungsdienst ist ein interner Dienst. Er bietet Schnittstellen zum prüfen von Syntax und Semantik. Dabei werden diejenigen spezifischen Dokumentformate unterstützt, die an den Außenschnittstellen anderer Dienste wie Signatur- und Verschlüsselungsdienst auftreten können.

Zugriffsberechtigungsdienst:

Der Zugriffsberechtigungsdienst ist ein interner Dienst. Er ermöglicht es, für vom Clientsystem aufgerufene Operationen eine Prüfung auf Zugriffsberechtigung für die von ihnen benötigten Ressourcen durchzuführen. Die Prüfung erfolgt direkt nach Aufruf einer Operation des Konnektors durch das Clientsystem und basiert auf den im Clientaufruf enthaltenen Parametern.

Der Zugriffsberechtigungsdienst definiert über ein Informationsmodell die erlaubten Zugriffsmöglichkeiten. Dabei werden im Informationsmodell Mandanten definiert und Clientsysteme sowie die vom Konnektor verwalteten externen Ressourcen (z. B. Kartenterminal mit Slots, Arbeitsplatz mit Signaturproxy, SMC-Bs etc.) zugeordnet.

Zertifikatsdienst:

Der Zertifikatsdienst bietet eine Schnittstelle zur Überprüfung der Gültigkeit von Zertifikaten an. Dies geschieht auf Grundlage des durch den Vertrauensanker (TSL-CA-Signer-Zertifikat und eine aktuelle, gültige TSL) aufgespannten Vertrauensraums sowie unter Berücksichtigung von aktuellen Statusinformationen (OCSP, CRL). Die Zertifikatsprüfung wird sowohl für nonQES- als auch für QES-Zertifikate unterstützt.

LDAP-Proxy:

Der Konnektor ermöglicht es Clientsystemen und Fachmodulen durch Nutzung des LDAP-Proxies Daten aus dem zentralen Verzeichnisdienst der TI-Plattform (VZD) mittels des Lightweight Directory Access Protocol abzufragen. Die Kommunikation erfolgt über das LDAPv3 Protokoll.

VSDM Fachmodul:

Das Fachmodul VSDM ist integraler Bestandteil des Konnektors und ermöglicht die Onlineprüfung und -aktualisierung der Versichertenstammdaten auf der eGK sowie die Bereitstellung und Pflege der Stammdaten des Versicherten in der Telematikinfrastruktur. Das VSDM Fachmodul ist dazu an die entsprechenden VSDM Fachdienste der TI, wie dem Versichertenstammdatendienst, dem Update Flag Service und dem Card Management System angebunden.

VAU-Client:

Der Konnektor unterstützt das ePA Fachmodule mit dem Aufbau einer sicheren Verbindung zur Vertrauenswürdigen Ausführungsumgebung (VAU) gemäß VAU-Kommunikationsprotokoll. Dabei wird ein sicherer Kanal auf HTTP-Anwendungsschicht zwischen dem Client und der VAU (Server) aufgebaut.

SGD-Client:

Der Konnektor unterstützt das ePA-Fachmodul bei der Nutzung der Schlüsselableitungsfunktionalität im Zusammenhang der ePA Fachanwendung. Der Gesamtablauf der Schlüsselableitungsfunktionalität für den Konnektor als Client ist aufgeteilt zwischen Basiskonnektor und Fachmodul. Die kryptographischen Vorgaben (u.a. Durchführung des ECDH, Schlüsselerzeugung, Ver- und Entschlüsselung, Signaturerzeugung und -prüfung) werden dabei durch den Konnektor realisiert.

1.3.6. Non-EVG hardware/software/firmware

Der EVG ist die Software des Netzkonnektor und Anwendungskonnektor inklusive UEFI Secure Boot Firmware für einen Einbox-Konnektor.

Anwendungshinweis 22: Die Hardware ist nicht Teil des EVGs

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

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

verwendet. Je Einbox-Konnektor werden dabei immer identische gSMC-Ks verbaut, die anhand der Identifikationsnummer (ICCSN) ermitteln werden können (siehe Handbuch [110]).

In der folgenden Tabelle sind die Mindestanforderungen an die HW Komponenten der Einbox-Konnektor Hardware beschrieben:

Komponente	**Beschreibung**
CPU	x86-64
RAM	8GB
Harddisk	16GB
Netzwerk	Zwei getrennte Netzwerkcontroller für WAN/LAN
Smartcard-Leser (für gSMC-K)	3 interne Smartcard-Leser für ID-000 Karten
RTC	Real Time Clock mit max. Drift von +/- 20ppm

Tabelle 2: Mindestanforderungen für Komponenten der Einbox-Konnektor Hardware

2. Postulat der Übereinstimmung

2.1. Common Criteria Konformität

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

Es wurden funktionale Sicherheitsanforderungen (FPT_EMS.1 und FIA_API.1, siehe Abschnitt 5.) definiert, die nicht in CC Teil 2 [5] enthalten ist. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [6] entnommen.

Daher ist dieses Security Target:

CC Teil 2 [5] erweitert (extended) und

CC Teil 3 [6] konform (conformant).

2.2. Security Target-Konformität

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

> Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Version 1.6 vom 30.03.2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das NK-PP [17] ist vollständig in diesem Schutzprofil enthalten.

2.3. Paket-Konformität

Das Security Target strebt die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponenten

- **AVA_VAN.3** (Resistenz gegen Angriffspotential „Enhanced-Basic“),
- **ADV_FSP.4** (Vollständige Funktionale Spezifikation),
- **ADV_TDS.3** (Einfaches Modulares Design),
- **ADV_IMP.1** (TSF-Implementierung),
- **ALC_TAT.1** (Wohldefinierte Entwicklungswerkzeuge) und
- **ALC_FLR.2** (Verfahren für Problemreports) an.

2.4. Begründung der Konformität

Das Security Target verwendet funktionale Sicherheitsanforderungen aus CC Teil 2 [5] sowie zwei funktionale Sicherheitsanforderung, die nicht in CC Teil 2 [5] enthalten ist, daher ist das Security Target CC Teil 2 erweitert (extended).

Das Security Target verwendet nur Anforderungen an die Vertrauenswürdigkeit aus CC Teil 3 [6], daher ist das Security Target CC Teil 3 konform (conformant).

Da das Security Target keine Konformität zu einem anderen Schutzprofil behauptet, können auch keine Widersprüche zwischen Schutzprofilen im EVG-Typ oder in der Definition des Sicherheitsproblems, der Sicherheitsziele und der Sicherheitsanforderungen auftreten.

Das zugrundeliegende Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, wie sie in CC Teil 3 [6] definiert ist, zusammen mit der Komponente AVA_VAN.3, um Schutz gegen „Enhanced-Basic“ Angriffspotenzial zu erreichen. Durch direkte und indirekte Abhängigkeiten der Komponente AVA_VAN.3 werden die Komponenten ADV_IMP.1 und ALC_TAT.1 aufgenommen und die Komponenten ADV_TDS.3 und ADV_FSP.4 augmentiert. Darüber hinaus wurde die Stufe EAL3 noch um die Komponente ALC_FLR.2 augmentiert, die keine Abhängigkeiten besitzt; für die Gründe dazu siehe Abschnitt 6.5. Das Security Target übernimmt die Vertrauenswürdigkeitsstufe des Schutzprofils. Damit sind alle Anforderungen an die Konformität erfüllt.

2.5. ST-Organisation

Der Aufbau dieses Security Targets folgt der Gliederung, des zugehörigen Schutzprofils („Schutzprofil 2: Anforderungen an den Konnektor, [16], BSI-CC-PP-0098“.

3. Definition des Sicherheitsproblems

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

Die Namensgebung der symbolischen Bezeichner für die im Folgenden definierten Bedrohungen, organisatorischen Sicherheitspolitiken sowie der Annahmen folgt der des zugrundeliegenden PP [16].

3.1. Werte

Zu schützende Werte sind zu schützende Informationen, Abläufe (Prozesse) oder dezentrale Ressourcen. Der Schutz erfolgt durch den EVG in Verbindung mit Maßnahmen in der Umgebung. Die Aufteilung in vom EVG bzw. von seiner Einsatzumgebung zu erfüllende Sicherheitsziele erfolgt in Kapitel 4.

3.1.1. Zu schützende Werte

Bei den zu schützenden Werten wird zwischen primären und sekundären Werten unterschieden, deren Definition aus [16] übernommen wurde:

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

3.1.1.1. Durch den Netzkonnektor zu schützende Werte

Im Folgenden sind die durch den Netzkonnktor zu schützenden Werte definiert. Diese wurden vollständig aus dem PP [16] entnommen und entsprechen den im Schutzprofil BSI-CC-PP-0097 [17] des Netzkonnektor definierten Werten.

Die **primären Werte** sind in der folgenden Tabelle 3 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze	Vertraulichkeit, Integrität, Authentizität	Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform werden zu schützende Daten der TI und der Bestandsnetze ausgetauscht. Unbefugte dürfen weder

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur-Plattform (beide Übertragungsrichtungen)		Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein. ⇒ **T.NK.local_EVG_LAN**, **T.NK.remote_EVG_LAN**, **T.NK.remote_EVG_WAN**, **T.NK.remote_VPN_Data**, A.NK.AK, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**, **T.NK.Zert_Prüf**, **T.NK.DNS**
zu schützende Nutzerdaten während der Übertragung zwischen Konnektor und sicherem Internet Service	Vertraulichkeit, Integrität, Authentizität	Beim Zugriff auf Internet-Dienste werden Nutzerdaten zwischen den lokalen Netzen der Leistungserbringer und dem sicheren Zugangspunkt zum Internet ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der angegebene Schutz der Authentizität bezieht sich auf die Tunnel-Endpunkte, nicht auf die im Tunnel übertragenen Daten. ⇒ **T.NK.local_EVG_LAN**, **T.NK.remote_EVG_LAN**, **T.NK.remote_EVG_WAN**, **T.NK.remote_VPN_Data**, A.NK.AK, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**, **T.NK.DNS**
zu schützende Daten der TI und der Bestandsnetze im Clientsystem	Vertraulichkeit, Integrität	Auf den Clientsystemen werden zu schützende Daten der TI und der Bestandsnetze vorgehalten. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten manipulieren können. ⇒ **T.NK.remote_EVG_LAN**, A.NK.phys_Schutz
in der zentralen Telematikinfrastruktur-Plattform gespeicherte zu schützende Daten der TI und der Bestandsnetze	Vertraulichkeit, Integrität	Werden zu schützende Daten der TI und der Bestandsnetze in der zentralen Telematikinfrastruktur-Plattform gespeichert, so dürfen diese, abhängig von ihrem Schutzbedarf (abhängig vom Fachdienst), auch dort nicht unbefugt eingesehen oder unbemerkt verändert werden können. ⇒ **T.NK.remote_VPN_Data**, A.NK.sichere_TI
Clientsystem, Anwendungskonnektor	Integrität	Manipulierte Clientsysteme oder Anwendungskonnektoren können dazu führen, dass zu schützende Daten der TI und der Bestandsnetze abfließen oder unautorisiert verändert werden.

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

Tabelle 3: Primäre Werte

Die primären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 1 aus dem NK-PP [17] bzw. aus dem zugrundeliegenden PP [16]

Die **sekundären Werte** sind in der folgenden Tabelle 4 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze im EVG	Vertraulichkeit, Integrität	Auch während der Verarbeitung im EVG müssen zu schützende Daten der TI und der Bestandsnetze gegen unbefugte Kenntnisnahme und Veränderung geschützt werden. ⇒ **T.NK.local_EVG_LAN**, , **T.NK.remote_EVG_LAN**, **T.NK.remote_EVG_WAN**
kryptographisches Schlüsselmaterial (während seiner Speicherung im EVG oder Verwendung durch den EVG)	Vertraulichkeit, Integrität, Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikations-partners sicherzustellen. ⇒ A.NK.phys_Schutz, **T.NK.local_EVG_LAN**, **T.NK.remote_EVG_WAN**, **T.NK.remote_EVG_LAN**, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**, **T.NK.Zert_Prüf**
Authentisierungs-geheimnisse (im EVG gespeicherte Referenzdaten und zum EVG über-tragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungs-geheimnissen (z. B. Passwort für Administrator-authentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (**T.NK.local_EVG_LAN**, **T.NK.remote_EVG_WAN**, **T.NK.remote_EVG_LAN**, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**)
Management-Daten (während ihrer Übertragung zum EVG)	Vertraulichkeit, Integrität und Authentizität	Wenn der EVG administriert wird, dürfen die administrativen Datenströme nicht eingesehen oder unbemerkt verändert werden können. ⇒ **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**
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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (**T.NK.local_EVG_LAN**, **T.NK.remote_EVG_WAN**, **T.NK.remote_EVG_LAN**, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**)
Sicherheits-Log-Daten (Audit-Daten)	Integrität, Verfügbarkeit	Der EVG muss Sicherheits-Log-Daten generieren, anhand derer Veränderungen an der Konfiguration des EVG nachvollzogen werden können (vgl. O.NK.Protokoll und FAU_GEN.1/NK.SecLog). Niemand darf Sicherheits-Log-Daten löschen oder verändern können. Wenn der für die Sicherheits-Log-Daten vorgesehene Speicherbereich aufgebraucht ist, können die Sicherheits-Log-Daten zyklisch überschrieben werden. Die Sicherheits-Log-Daten müssen auch zum Nachweis der Aktivitäten von Administratoren verwendet werden können. ⇒ **T.NK.remote_EVG_WAN**, **T.NK.remote_EVG_LAN**, **T.NK.local_EVG_LAN**, **T.NK.local_admin_LAN**, **T.NK.remote_admin_WAN**, **T.NK.counterfeit**
Systemzeit	Verfügbarkeit, Gültigkeit	Der EVG muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern synchronisieren. Die Zeit wird für die Prüfung der Gültigkeit von VPN-Zertifikaten sowie für die Erzeugung von Zeitstempeln in Sicherheits-Log-Daten oder Audit-Daten verwendet. ⇒ **T.NK.TimeSync**

Tabelle 4: Sekundäre Werte

Die sekundären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 2 aus dem NK-PP [17] bzw. aus dem zugrundeliegenden PP [16]

3.1.1.2. Durch den Anwendungskonnektor zu schützende Werte

Die **primären Werte** sind in der folgenden Tabelle 5 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Nutzerdaten und Metadaten bei der Übertragung zwischen Clientsystem und EVG	Integrität, Authentizität, Vertraulichkeit	Die Daten bzw. Dokumente, die von den Clientsystemen im lokalen Netz der Leistungserbringer dem Konnektor zur Bearbeitung übergeben werden bzw. die Ergebnisse der Bearbeitung durch den Konnektor dürfen bei der Übermittlung weder verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. ⇒ T.AK.LAN.CS, **T.AK.Mani.Client**, **T.AK.MissbrauchKarte**, **T.AK.Fehlbedienung**, A.AK.Konnektor
Nutzerdaten und Metadaten bei der Übertragung zwischen EVG und Fachdiensten sowie PKI-Diensten der TI	Integrität, Authentizität, Vertraulichkeit	Die Daten bzw. Dokumente, die vom EVG zur Bearbeitung an Fachdienste übergeben werden, bzw. die Ergebnisse der Bearbeitung durch die Fachdienste dürfen bei der Übermittlung weder verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. PKI-Daten, die der EVG von PKI-Diensten der TI empfängt, dürfen nicht manipuliert werden. ⇒ T.AK.WAN.TI, **T.AK.Kanal_Missbrauch**, **T.AK.Mani.TI**, **T.AK.Mani.ExternerDienst**, A.AK.Konnektor, A.AK.sichere_TI
Nutzerdaten und Metadaten bei der Übertragung zwischen EVG und Fachmodulen	Integrität, Authentizität, Vertraulichkeit	Die Daten bzw. Dokumente, die vom EVG zur Bearbeitung an Fachmodule im Konnektor übergeben werden bzw. die Ergebnisse der Bearbeitung durch die Fachmodule dürfen bei der Übermittlung weder verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. ⇒ T.AK.LAN.CS, A.AK.Konnektor
Nutzerdaten und Metadaten innerhalb des EVG	Integrität, Vertraulichkeit	Die Daten bzw. Dokumente, die innerhalb des EVG bearbeitet, gespeichert oder übertragen werden, dürfen

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
		nicht unautorisiert verändert oder eingesehen werden.[11] ⇒ **T.AK.Mani.EVG**, **T.AK.Mani.TI**, A.AK.Konnektor, A.AK.phys_Schutz
VAU-/SGD-Inhaltsdaten	Integrität, Authentizität, Vertraulichkeit	Nutzerdaten und Metadaten, die vom EVG zur Vearbeitung in die VAU-Instanz des ePA-Aktensystems (betrifft ePA-Metadaten und ePA-Aktenschlüssel) bzw. in das SGD-HSM (betrifft SGD-AES-Schlüssel) übergeben werden, bzw. von diesen empfangen werden, dürfen bei der Übermittlung weder unbemerkt verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. ⇒ OSP.AK.VAUSGD

Tabelle 5: primäre Werte des Anwendungskonnektors

Die primären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 3 aus dem zugrundeliegenden PP [16]

Die **sekundären Werte** sind in der folgenden Tabelle 6 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Metadaten und Authentisierungsgeheimnisse bei der Übertragung zwischen EVG und Kartenterminal	Integrität, Vertraulichkeit	Die Daten und Authentisierungsgeheimnisse bei der Übertragung zwischen Konnektor und Kartenterminal dürfen bei der Übermittlung weder verändert noch unbefugt eingesehen werden. ⇒ T.AK.DTBS, T.AK.VAD, T.AK.LAN.eHKT, **T.AK.Kanal_Missbrauch**, A.AK.Konnektor
Metadaten und Authentisierungs-geheimnisse bei der Bearbeitung im Kartenterminal	Integrität, Vertraulichkeit	Die Daten und Authentisierungsgeheimnisse während der Bearbeitung und Zwischenspeicherung innerhalb des Kartenterminals dürfen nicht unautorisiert verändert oder eingesehen werden. ⇒ T.AK.DTBS, T.AK.VAD, T.AK.Mani.Terminal, A.AK.Konnektor, A.AK.Cardterminal_eHealth

[11] Hierzu die Daten bei der Übertragung zur gSMC-K

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Nutzerdaten und Metadaten bei der Übertragung zwischen EVG und (externer) Chipkarte	Integrität, Authentizität, Vertraulichkeit	Die Daten und Metadaten bei der Übertragung zwischen Konnektor und externer Chipkarte dürfen bei der Übermittlung weder verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. ⇒ T.AK.DTBS, T.AK.VAD, **T.AK.Kanal_Missbrauch**, A.AK.Konnektor, A.AK.Cardterminal_eHealth, A.AK.SMC, A.AK.QSCD, A.AK.Chipkarteninhaber
Nutzerdaten, Authentisierungs-geheimnisse, kryptografische Daten und Metadaten bei der Bearbeitung und Speicherung auf der (externen) Chipkarte	Integrität, Vertraulichkeit	Die Daten, Authentisierungsgeheimnisse und kryptografische Daten während der Bearbeitung und Speicherung innerhalb der externen Chipkarte dürfen nicht unautorisiert verändert oder eingesehen werden. ⇒ T.AK.Mani.Chipkarte, **T.AK.MissbrauchKarte**, A.AK.SMC, A.AK.QSCD, A.AK.Chipkarteninhaber
Kryptografische Daten bei der Bearbeitung bzw. Nutzung oder Speicherung im EVG	Integrität, Vertraulichkeit	Das im EVG erzeugte, verwendete oder gespeicherte Schlüsselmaterial darf nicht unautorisiert verändert oder eingesehen werden. ⇒ **T.AK.Mani.EVG**, A.AK.Konnektor, A.AK.Env_Arbeitsplatz, A.AK.phys_Schutz
Management-Daten bei der Übertragung zum EVG	Integrität, Authentizität, Vertraulichkeit	Bei der Administration des EVG dürfen administrative Daten während der Übermittlung nicht unbefugt modifiziert oder eingesehen werden. Zudem dürfen nur authentisierte Partner kommunizieren. ⇒ T.AK.LAN.CS, **T.AK.LAN.Admin**, T.AK.Mani.AdminKonsole,A.AK.Konnektor, A.AK.Admin_EVG
Management-Daten bei der Speicherung und Bearbeitung im EVG	Integrität	Management-Daten (z. B. Konfigurationsdaten) des EVG dürfen nicht unbemerkt verändert werden können. ⇒ T.AK.Mani.AdminKonsole, **T.AK.Fehlbedienung**, A.AK.Konnektor, A.AK.Admin_EVG, A.AK.phys_Schutz
Authentisierungs-geheimnisse bei der	Integrität, Vertraulichkeit	Die Vertraulichkeit und Integrität von Authenti-sierungsgeheimnissen (z. B. Passwort für

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Speicherung und Bearbeitung im EVG		Administratorauthentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ **T.AK.Mani.EVG**, A.AK.Konnektor, A.AK.Admin_EVG, A.AK.phys_Schutz
Sicherheits-Log-Daten (Audit-Daten)	Integrität, Verfügbarkeit	Der EVG muss Sicherheits-Log-Daten generieren, anhand derer Veränderungen an der Konfiguration des EVG nachvollzogen werden können. Diese Daten dürfen nicht modifiziert oder unautorisiert gelöscht werden. ⇒ A.AK.Konnektor, A.AK.Admin_EVG, A.AK.phys_Schutz
Systemzeit	Integrität, Verfügbarkeit	Der EVG muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern synchronisieren. ⇒ **T.AK.Mani.ExternerDienst**, A.AK.Konnektor, A.AK.phys_Schutz
Software und Hardware des EVG	Integrität	Gelingt es einem Angreifer, die Integrität des EVG zu verletzen, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ A.AK.Konnektor, A.AK.phys_Schutz

Tabelle 6: sekundäre Werte des Anwendungskonnektors

Die primären Werte, deren Schutzbedarf und das daraus abgeleitete Bedrohungspotential bzw. erforderlichen Annahmen entsprechen denen aus der Tabelle 4 aus dem zugrundeliegenden PP [16]

Der für die Signaturerstellung notwendige Signaturschlüssel (SCD[12]) ebenso wie die Authentisierungsreferenzdaten (SRAD[13]) des Signaturschlüssel-Inhabers befinden sich in der qualifizierten Signaturerstellungseinheit (QSEE) und werden durch diese geschützt.

3.1.2. Benutzer des EVG

3.1.2.1. Benutzer des Netzkonnektors

Die folgenden Benutzer des Netzkonnektors sind dem Schutzprofil BSI-CC-PP-0098 [16], Kapitel 3.1.2.1 entnommen.

In der Einsatzumgebung des EVGs gibt es folgende externe Einheiten:

[12] Englisch: signature-creation data

[13] Englisch: signatory reference authentication data

Benutzer des Netzkonnektors	Beschreibung
AK	Anwendungskonnektor
VPN-TI	Entfernter VPN-Konzentrator, der den Zugriff auf die Telematikinfrastruktur vermittelt
VPN-SIS	Entfernter VPN-Konzentrator, der den sicheren Zugriff auf das Internet realisiert
DNS-ext	(externer) DNS-Server für den Namensraum Internet
Zeit-ext	(externer) Zeit-Server des Zugangsnetzproviders
CS	Clientsystem
TSL/CRL	Bereitstellungspunkte für TSL und CRL
Admin	**NK-Admin** oder auch **NK-Administrator**: Administrator des Netzkonnektors
Angreifer	Ein Angreifer

Tabelle 7: Benutzer des Netzkonnektors

Der **Admin** authentisiert sich gegenüber dem Konnektor (siehe O.NK.Admin_EVG). Der EVG unterscheidet intern zwischen den drei Administrator-Rollen *local administrator*, *remote administrator* und *super administrator*. Siehe auch Anwendungshinweis 36:.

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

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

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

Für den **Leistungserbringer** sind die Leistungen des NK transparent, er arbeitet mit dem Clientsystem. Sofern er Einstellungen des NK verändert, agiert er in der Rolle des **NK-Administrators**. Deshalb sind Leistungserbringer bzw. HBA-Inhaber nicht gesondert als eigene externe Einheiten modelliert. Auch ein Leistungserbringer könnte grundsätzlich in der Rolle des Angreifers auftreten: Innerhalb des NK gibt es Geheimnisse (z. B. Sitzungsschlüssel des VPN-Kanals), die auch ein Leistungserbringer nicht kennen soll. Versucht ein Leistungserbringer, Kenntnis von diesen Geheimnissen zu erlangen, kann dies als Angriff

betrachtet werden. Beim Leistungserbringer gilt jedoch folgende Einschränkung: Weder der NK noch der Anwendungskonnektor können gegen den Willen eines Leistungserbringers Datenschutzanforderungen durchsetzen, solange Clientsysteme dies nicht unterstützen. Daher werden solche potentiellen Angriffe eines Leistungserbringers hier **nicht** betrachtet (das Verhindern solcher Angriffe ist nicht Bestandteil der EVG-Sicherheitspolitik). Im Umfeld des Konnektors wird der Leistungserbringer als vertrauenswürdig angesehen, da er üblicherweise auch die Erfüllung des Umgebungsziels OE.NK.phys_Schutz sicherstellen muss.

3.1.2.2. Objekte des Netzkonnektors

Die folgenden Benutzer des Netzkonnektors sind dem Schutzprofil BSI-CC-PP-0098 [16], Kapitel 3.1.2.2 entnommen.

Es werden die folgenden Objekte betrachtet:

Objekte des Netzkonnektors	**Beschreibung**
CS-Daten	Lokal beim Leistungserbringer (in Clientsystemen im LAN) gespeicherte zu schützende Daten der TI und der Bestandsnetze
VPN-Daten-TI	zu schützende Daten der TI und der Bestandsnetze während des Transports zwischen NK und VPN-K der Telematikinfrastruktur
VPN-Daten-SIS	*zu schützende Nutzerdaten* während des Transports zwischen NK und VPN-SIS
TI-Daten	Entfernt in den Datenbanken der Telematikinfrastruktur bzw. den Bestandsnetzen gespeicherte zu schützende Daten der TI und der Bestandsnetze

Es wird davon ausgegangen, dass die VPN-Daten durch den zwischen NK und VPN-Konzentratoren implementierten sicheren Kanal (d.h. durch das VPN) geschützt werden und dass die TI-Daten nur in verschlüsselter Form gespeichert vorliegen (z. B. eVerordnung) (siehe A.NK.sichere_TI in Abschnitt 3.4). Die Sicherheit der Clientsysteme ist nicht Gegenstand der Betrachtung.

3.1.2.3. Benutzer des Anwendungskonnektors

Über die in Abschnitt 3.1.2.1 genannten Benutzer unterscheidet der Konnektor die folgenden Benutzer, d.h. externe Instanzen, die mit dem EVG kommunizieren (vergl. CC Teil 1 [4], Kap. 4). Die für sie handelnden Subjekte sind im Kapitel 6.1.2 beschrieben.

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
Administrator	Benutzer für administrative Funktionen des EVG. Der Administrator benutzt eine gesonderte Management-schnittstelle (vergl. [27], Kap. 4.3).	**Identität des Benutzers**: Daten zur Identifizierung des Benutzers mit Administratorrechten. **Authentisierungsreferenzdaten**: individuelles Passwort des Benutzers mit Administratorrechten oder andere Authentisierungsreferenzdaten gemäß FIA_UAU.5.
Clientsystem	Komponente mit einem Benutzerinterface für fachliche Funktionalität, die über das LAN des Leistungserbringers mit dem Konnektor verbunden ist. Die Primärsysteme der Leistungs-erbringer sind spezielle Client-systeme und umfassen die Praxis-verwaltungssysteme für Ärzte, Zahnärzte und Psychotherapeuten, die Krankenhausinformations-systeme der Krankenhäuser und die Apothekenverwaltungssysteme der Apotheker und stellen die Anwen-dungsprogramme für die Leistungs-erbringer und Versicherten zur Verfügung. Ohne Nutzung eines TLS-Kanals kann der EVG nicht zwischen einer beliebigen Komponente im LAN und einem Clientsystem unterscheiden.	Bei Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: Öffentlicher Schlüssel Ohne Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: keine Sicherheitsattribute
Fachmodul	Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablauf-definitionen der TI-Plattform.	**ServiceInformation:** XML-Datei zur Beschreibung der Dienste des Fachmoduls gemäß ServiceInformation.xsd
VPN-Konzentrator der TI	Der VPN-Konzentrator der Telematikinfrastruktur ist ein	

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
	Sammelpunkt für mehrere VPN-Verbindungen.	
VPN-Konzentrator des SIS	Der VPN-Konzentrator der Internetserviceproviders ist ein Sammelpunkt für mehrere VPN-Verbindungen zur Erbringung sicherer Internetdienstleistungen.	
Benutzer des Clientsystems	Der Benutzer des Clientsystems als logische Schnittstelle des EVG. Er wird durch den EVG identifiziert. Der Benutzer des Clientsystems kann durch die korrekte Authentisierung gegenüber der zu benutzenden Chipkarte für die Benutzung des EVG autorisiert werden. Die Gültigkeit einer Autorisierung kann für EVG-Funktionen in Abhängigkeit von der verwendeten Chipkarte konfiguriert werden. Für die qualifizierte elektronische Signatur muss eine Autorisierung des Benutzers für das Signieren eines jeden einzelnen Stapels der Stapelsignatur durch die qualifizierte Signaturerstellungseinheit (HBA) erfolgen. Bei der Komfortsignatur erfolgt die Autorisierung des Benutzers durch den HBA jeweils für eine HBA-Kartensitzung bei Aktivierung des Komfortsignaturmodus. Für jede Signaturerstellung in der HBA-Kartensitzung mittels Komfortsignatur authentisiert sich das Clientsystem dann mit einer eindeutigen Identifikationsnummer.	**Identität des Clientsystem-Benutzers**: Datum zur Identifizierung des Benutzers. Diese Identität muss den Chipkarten HBA, SMC-B und ggf. eGK zugeordnet werden können. **Autorisierungsstatus**: Status der Zuordnung des Benutzers des Clientsystems zu dem Authentisierungsstatus der Chipkarte in Abhängigkeit von der gewünschten Funktion. Werte: - „nicht autorisiert“: Zuordnung nicht durch Chipkarte bestätigt, - „autorisiert“: Zuordnung durch Chipkarte bestätigt. **Arbeitsplatz**: Identität des gegenwärtigen Arbeitsplatzes des Benutzers.

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
Signierender	Inhaber des Signaturschlüssels für die Erstellung einer Signatur.	**Identität des Signaturschlüssel-Inhabers**: Identität des Signaturschlüssel-Inhabers, die im Zertifikat des Signaturschlüssels angegeben ist, das der Signatur zugrunde liegt.
eHealth-Kartenterminal	eHealth-Kartenterminal im lokalen Netz des Leistungserbringers, das über eine gSMC-KT verfügt und mit dem EVG gepaart wird bzw. ist (s. [38] Kap. 3.7).	**Identität**: Umfasst die - ID.SMKT.AUT der gSMC-KT des eHealth-Kartenterminals, - physische Adresse im LAN-LE. **Authentisierungsreferenzdaten**: Authentisierungsreferenzdaten zur Authentisierung der eHealth-Kartenterminals zum Aufbau des TLS-Kanals; umfasst das Zertifikat in EF.C.SMKT.AUT der gSMC-KT, die zum Pairing benutzt wurde, und das Pairing-Geheimnis ShS.KT.AUT. **Arbeitsplatz**: Arbeitsplatz bzw. Arbeitsplätze, denen das eHealth-Kartenterminal zugeordnet ist, mit Angabe, ob es für den Arbeitsplatz lokales oder entferntes eHealth-Kartenterminal ist. Ein eHealth-Kartenterminal kann auch keinem Arbeitsplatz zugeordnet sein.
gSMC-KT	Chipkarte gSMC-KT als Sicherheitsmodule für eHealth-Kartenterminals	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel in den Zertifikaten - C.SMKT.AUT als gSMC-KT. - C.SMC.AUTD_RPS_CVC mit CHAT als PIN-Sender.

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
Benutzer des EVG am eHealth-Kartenterminal	Benutzer des EVG, der das eHealth-Kartenterminal als Benutzerschnittstelle nutzt, d. h. der vom EVG generierte Anzeigen liest und Daten über die Tatstatur des eHealth-Kartenterminals eingibt, die durch das eHealth-Kartenterminal entsprechend den SICCT-Kommandos des EVG verarbeitet werden.	Keine
eGK	Chipkarte, die durch den EVG identifiziert und sich gegenüber dem anderen Chipkarten mit CVC und privaten Schlüssel oder davon abgeleiteten symmetrischen Schlüsseln als eGK gegenüber CMS oder VSDM-Fachdienst authentisiert.	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: - öffentlicher Schlüssel und CHA, bzw. CHAT in dem CVC C.eGK.AUT_CVC als eGK gegenüber anderen Chipkarten, - SK.CMS als eGK gegenüber einem CMS, - SK.VSD als eGK gegenüber einem VSDM-Fachdienst.
HBA	Chipkarte, die durch den EVG identifiziert und sich gegenüber dem EVG mit CVC und privaten Schlüssel oder davon abgeleiteten symmetrischen Schlüsseln als HBA authentisiert. Der HBA dient als QSEE mit Signaturschlüssel PrK.HP.QES, Träger des Entschlüsselungsschlüssels und PIN-Empfänger.	**Identität**: - ICCSN - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten und Entschlüsselungsschlüsselinhabers für zu verschlüsselnde Daten. **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten - C.HPC.AUTR_CVC als HBA gegenüber SMC und eGK, - C.HPC.AUTD_SUK_CVCals QSEE für Stapelsignatur und PIN-Empfänger

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
		- C.HP.ENC als Träger des dazu gehörigen Entschlüsselungsschlüssels PrK.HP.ENC. **Optionale Authentisierungsreferenzdaten:** - PuK.RCA.ADMINCMS.CS.E256 des CMS gegenüber einem HBA. - SK.CMS.AES128 bzw. SK.CMS.AES256 und SK.CUP.AES128 bzw. SK.CUP.AES256 zur gegenseitigen Authentisierung zwischen CAMS und HBA.
HBAx	Sammelbegriff für den HBA, den HBA-qSig und den ZOD-2.0.	**Identität**: - ICCSN - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten und Entschlüsselungsschlüsselinhabers für zu verschlüsselnde Daten.
SMC-B	Chipkarte, die durch den EVG identifiziert und sich gegenüber dem EVG mit CVC und privaten Schlüssel oder davon abgeleiteten symmetrischen Schlüsseln als SMC-B authentisiert. Die SMC-B kann in Übereinstimmung mit den Rechten des Kartenhalters als PIN-Empfänger, Träger des privaten Entschlüsselungsschlüssels, Träger des privaten Signaturschlüssels, des privaten Schlüssels zur CVC-Authentisierung gegenüber der eGK und des privaten Schlüssels zur X.509-Authentisierungsschlüssels gegenüber externen Gegenstellen verwendet werden.	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten: - C.SMC.AUTR_CVC als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC als SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung. **Optionale Authentisierungsreferenzdaten:** - PuK.RCA.ADMINCMS.CS.E256 des CMS gegenüber einer SMC-B.

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
		- SK.CMS.AES128 bzw. SK.CMS.AES256 und SK.CUP.AES128 bzw. SK.CUP.AES256 zur gegenseitigen Authentisierung zwischen CAMS und SMC-B.
HSM-B	Hardwaresicherheitsmodul, der durch den EVG identifiziert und sich gegenüber dem EVG mit CVC und privaten Schlüssel als SM-B authentisiert. Der HSM-B wird als Träger des privaten Entschlüsselungsschlüssels, Träger des privaten Signaturschlüssels, des privaten Schlüssels zur CVC-Authentisierung gegenüber der eGK und des privaten Schlüssels zur X.509-Authentisierungsschlüssels gegenüber externen Gegenstellen verwendet. Ein HSM-B kann mehrere SMC-Bs repräsentieren.	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten: - C.SMC.AUTR_CVC als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC als SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung,.

Tabelle 8: Benutzer des Anwendungskonnektors

Benutzer	Beschreibung
Signaturschlüssel-Inhaber (HBA)	Der Signaturschlüssel-Inhaber ist der legitime Benutzer des Signaturschlüssels eines HBA als qualifizierte Signaturerstellungseinheit (Authentisierung mit PIN.QES)
Kartenhalter des HBA	HBA-Inhaber für alle Funktionen des HBA außer der Signaturfunktion (Authentisierung mit PIN.CH)
Kartenhalter der SMC-B	Kartenhalter für Funktionen der SMC-B (Authentisierung mit PIN.SMC)
Versicherter	eGK-Inhaber für die Authentisierung, die Entschlüsselungsfunktion und die Nachrichtenauthentisierung (Authentisierung mit PIN.CH oder Referenz-PIN)
KT-Benutzer	Benutzer des eHealth-Kartenterminals.

Tabelle 9: Benutzer anderer Komponenten in der IT-Umgebung

3.2. Bedrohungen

3.2.1. Gegen den Netzkonnektor gerichtete Bedrohungen

3.2.1.1. Auswahl der betrachteten Bedrohungen

Eine Motivation der in Abschnitt 3.2.1.2 beschriebenen Bedrohungen sowie eine Beschreibung der möglichen Angriffspfade ist dem PP [17], Abschnitt 3.3.1 zu entnehmen.

Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen sind:

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

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

3.2.1.2. Liste der Bedrohungen

Ein detaillierte motivation der Bedrohungen findet sich im PP [17], Abschnitt 3.2.1.2. In den folgenden Tabellen werden nur die konkreten Bedrohungen wiedergegeben. Diese wurden unverändert aus dem PP übernommen.

T.NK.local_EVG_LAN

Ein Angreifer dringt lokal in die Räumlichkeiten des Leistungserbringers ein und greift den Netzkonnektor über dessen LAN-Schnittstelle an. Ziel bzw. Motivation des Angriffs ist es,

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

Für diesen Angriff kann der Angreifer sowohl vorhandene IT-Systeme im LAN des Leistungserbringers nutzen als auch eigene (z. B. Notebook, Netbook, PDA[14], Smartphone/Handy) mitbringen.

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

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

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

[14] Personal Digital Assistant

T.NK.remote_EVG_WAN

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

T.NK.remote_EVG_LAN

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

Hierzu werden in [17], Abbildung 4 zwei Angriffspfade unterschieden:

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

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

Einen Spezialfall dieses Angriffs (Angriffspfad 3.1 oder 3.2) stellt das Szenario dar, dass ein IT-System im LAN vom Transportnetz bzw. Internet (WAN) aus mit bösartigem Code verseucht wird und in der Folge Angriffe gegen den Konnektor an dessen LAN-seitiger Schnittstelle vornimmt. Ein IT-System im LAN könnte vom Transportnetz aus mit bösartigem Code verseucht werden, wenn der Netzkonnektor keine effektive Netztrennung[15] zwischen WAN und LAN leistet.

Betroffene zu schützende Werte sind:

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

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

T.NK.remote_VPN_Data

Ein Angreifer aus dem Transportnetz hört Daten ab oder manipuliert Daten unbemerkt, die zwischen dem Konnektor und der zentralen Telematikinfrastruktur-Plattform (Angriffspfad 4.2, Abbildung 4 aus [16]) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1, Abbildung 4 aus [16]) übertragen werden.

Dies umfasst folgende Aspekte:

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

Betroffene zu schützende Werte sind:

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

T.NK.local_admin_LAN

Ein Angreifer dringt lokal in die Räumlichkeiten des Leistungserbringers ein und verändert (im Rahmen lokaler Administration) sicherheitsrelevante Einstellungen des Netzkonnektors. Dies kann dem Angreifer einerseits dadurch gelingen, dass der Netzkonnektor das Verändern von sicherheitsrelevanten Einstellungen nicht hinreichend schützt (im Sinne einer Zugriffskontrolle), oder andererseits dadurch, dass sich ein Angreifer erfolgreich als Administrator ausgeben und mit dessen Berechtigungen agieren kann (im Sinne einer

Authentisierung/Autorisierung). Ziel des Angreifers kann es sein, Sicherheitsfunktionen des Netzkonnektors zu deaktivieren (z. B. Abschalten der Verschlüsselung auf dem VPN-Kanal oder Erlauben bzw. Erzwingen kurzer Schlüssellängen), die Integrität des Netzkonnektors selbst zu verletzen, Schlüssel auszulesen, um damit Zugriff auf geschützte Daten zu erhalten oder auch die Grundlagen für weiteren Missbrauch zu legen – etwa durch Einspielen schadhafter Software, welche Kopien aller vom Netzkonnektor übertragenen Daten am VPN-Tunnel vorbei zum Angreifer spiegelt.

Diese Bedrohung umfasst auch folgende Aspekte:

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

T.NK.remote_admin_WAN

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

Diese Bedrohung umfasst auch folgende Aspekte:

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

T.NK.counterfeit

Ein Angreifer bringt gefälschte Netzkonnektoren in Umlauf, ohne dass dies vom VPN-Konzentrator erkannt wird[16]. Der Angriff kann durch den unbemerkten Austausch eines bereits im Einsatz befindlichen Geräts erfolgen – wozu in der Regel ein Eindringen in die Räumlichkeiten des Leistungserbringers erforderlich ist – oder bei der Erstauslieferung durchgeführt werden. Der Angreifer verfolgt dieselben Ziele wie unter T.NK.local_admin_LAN besprochen.

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

T.NK.Zert_Prüf

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

T.NK.TimeSync

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

T.NK.DNS

Ein Angreifer manipuliert aus dem Transportnetz heraus Antworten auf DNS-Anfragen zu externen DNS-Servern. Dies kann einerseits Anfragen des Netzkonnektors betreffen, wenn dieser vor dem Aufbau von VPN-Kanälen die Adresse des VPN-Konzentrators der TI oder des SIS ermitteln will. Im Ergebnis wird keine oder eine falsche Adresse ausgeliefert, so dass der Netzkonnektor ggf. die VPN-Verbindung zu einem gefälschten Endpunkt aufbaut, der

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

beispielsweise eine gefälschte zentrale TI-Plattform vorspiegelt. Dadurch werden die zu schützende Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur-Plattform bedroht. Andererseits können gefälschte DNS-Antworten auch beim Internet-Zugriff von Clientsystemen der Leistungserbringer auftreten. In einem solchen Szenario könnte der Angreifer den Zugriff der Clientsysteme auf manipulierte Systeme umleiten (Wert: zu schützende Nutzerdaten während der Übertragung zwischen Konnektor und sicherem Internet Service), um Clientsysteme mit bösartigem Code zu infizieren, der dann das lokale Netz, den Netzkonnektor und die zu schützenden Werte bedroht.

3.2.2. Gegen den Anwendungskonnektor gerichtete Bedrohungen

Über die in Abschnitt 3.2.1 genannten Bedrohungen für den Netzkonnektor hinaus werden die folgenden weiteren Bedrohungen gegen die zu schützenden Werte des Anwendungskonnektors definiert. In den folgenden Tabellen werden die Bedrohungen wiedergegeben. Die Bedrohungen wurden unverändert aus dem PP [17] übernommen.

3.2.2.1. Kommunikation

T.AK.LAN.CS	Datenübertragung im LAN abhören und/oder manipulieren

Ein Angreifer hört im LAN zwischen dem Konnektor (inkl. Fachmodulen) und einem Clientsystem übertragene Daten (zu schützende Daten) ab und erhält so Kenntnis dieser Daten und/oder manipuliert diese Daten.

Ein Angreifer gibt sich dem Konnektor (inkl. Fachmodulen) gegenüber als ein rechtmäßiges Clientsystem aus (Vortäuschen einer falschen Identität).

Diese Bedrohungen beziehen sich auf die Datenübertragung in beiden Richtungen, also sowohl vom Konnektor (inkl. Fachmodulen) zu einem Clientsystem als auch von einem Clientsystem zum Konnektor (inkl. Fachmodulen).

Anwendungshinweis 23: Die komplementäre Bedrohung des Vortäuschens einer falschen Konnektor-Identität gegenüber einem Clientsystem muss durch eine erzwungene Authentisierung des Konnektors durch das Clientsystem abgewehrt werden und stellt somit keine Bedrohung gegen den Konnektor, **sondern** gegen das Clientsystem dar. Abhängig von dessen Konfiguration kann der Konnektor die Abwehr dieser Bedrohung unterstützen, indem er sich selbst gegenüber Clientsystemen authentisiert. Daher wurde in T.AK.LAN.CS die Formulierung „in beiden Richtungen“ verwendet.

T.AK.LAN.Admin	Abhören von Daten bei Adminstration

Ein Angreifer hört im LAN zwischen dem Konnektor und der Administrationskonsole übertragene Daten ab und erhält so Kenntnis dieser Daten und/oder manipuliert diese Daten

(Management-Daten bei der Übertragung zum EVG). Weiterhin können mitgeschnittene und ggf. modifizierte Daten zu einem späteren Zeitpunkt erneut zum EVG geschickt werden, um auf diese Weise unautorisiert administrative Funktionen des EVG aufzurufen.

T.AK.WAN.TI Datenübertragung im WAN abhören und/oder manipulieren

Ein Angreifer hört im Transportnetz (WAN) bzw. Zugangsnetz zwischen dem EVG und einem Fachdienst übertragene Daten (zu schützende Daten) ab und erhält so Kenntnis dieser Daten und/oder manipuliert diese Daten.

Ein Angreifer gibt sich einem Kommunikationspartner gegenüber als der rechtmäßige andere Kommunikationspartner aus (Vortäuschen einer falschen Identität).

Diese Bedrohungen beziehen sich auf die Datenübertragung in beiden Richtungen, also sowohl vom EVG zu einem Fachdienst als auch von einem Fachdienst zum EVG.

Anwendungshinweis 24: Analog zu Anwendungshinweis 23: gilt: Die komplementäre Bedrohung des Vortäuschens einer falschen Konnektor-Identität gegenüber einem Fachdienst muss durch den Fachdienst (erzwungene Authentisierung des Konnektors) abgewehrt werden und stellt damit also keine Bedrohung gegen den Konnektor, sondern gegen den Fachdienst dar. Der Konnektor unterstützt jedoch die Abwehr dieser Bedrohung, indem er sich selbst gegenüber dem Fachdienst authentisiert. Daher wurde in T.AK.WAN.TI die Formulierung „in beiden Richtungen“ verwendet.

T.AK.Kanal_Missbrauch Missbrauch bestehender Kommunikationskanäle

Ein Angreifer kann bestehende Kommunikationskanäle missbrauchen. Ein Angreifer versucht, in bestehende Kommunikationskanäle, etwa zwischen EVG und eHealth-Kartenterminal, zwischen EVG und Chipkarte oder zwischen EVG und Systemen der zentralen TI-Plattform, eigene Daten einzufügen, um unautorisiert Einfluss auf die Funktionalität des EVG oder auf zu schützende Daten zu nehmen.

3.2.2.2. Terminaldienst

T.AK.LAN.eHKT Abhören/Manipulieren der Datenübertragung zwischen dem Konnektor und den eHealth-Kartenterminals

Ein Angreifer hört im LAN zwischen dem Konnektor und einem eHealth-Kartenterminal übertragene Daten ab oder manipuliert diese Daten. Ein Angreifer gibt sich dem Konnektor gegenüber als ein rechtmäßiges eHealth-Kartenterminal aus (Vortäuschen einer falschen Identität). Diese Bedrohungen beziehen sich auf die Datenübertragung in beiden Richtungen, also sowohl vom Konnektor zu einem eHealth-Kartenterminal als auch von einem eHealth-

Kartenterminal zum Konnektor. Durch diese Bedrohung können Daten der Chipkarten und die Konnektor/eHKT-Kommunikation kompromittiert oder manipuliert werden.

3.2.2.3. Chipkartendienst

T.AK.VAD	Abhören/Manipulieren von Authentisierungsverifikationsdaten

Ein Angreifer versucht die VAD (d.h. die PIN oder PUK) eines Chipkartenbenutzers zu kompromittieren oder zu manipulieren. Ein Angreifer versucht insbesondere, die VAD bei der vom EVG gesteuerten entfernten PIN-Eingabe während der Übertragung zwischen dem PIN-Terminal und der Chipkarten-Terminal oder über das lokale Netz abzuhören oder zu manipulieren.

3.2.2.4. Signaturdienst

T.AK.DTBS	Einfügen/Manipulieren von zu signierenden Daten

Ein Angreifer kann Daten ohne die oder entgegen der Intention des Signaturschlüssel-Inhabers durch die qualifizierte Signaturerstellungseinheit oder andere Chipkarten signieren lassen. Dies kann durch Einfügen, Veränderung oder Ersetzen von zu signierenden Daten in einem Stapel zu signierender Daten bei der Übertragung zwischen Konnektor und Chipkarte (HBA bzw. SMC-B) erfolgen.

3.2.2.5. Manipulation und Missbrauch

T.AK.Mani.EVG	Manipulation des EVG

Ein Angreifer mit Zugriff auf den EVG oder auf Update-Daten für den EVG manipuliert Anteile des EVG, um Zugriff auf zu schützende Daten (Nutzerdaten, Metadaten, kryptographisches Schlüsselmaterial, Authentisierungsdaten) zu erlangen bzw. diese zu modifizieren.

T.AK.Mani.Client	Manipulation von Clientsystemen

Ein Angreifer mit Zugriff auf Clientsysteme manipuliert Clientsysteme, so dass durch unsachgemäße oder unautorisierte Nutzung der Dienste des EVG zu schützende Nutzer- und Metadaten offengelegt oder manipuliert werden können. Der Angriff kann auch durch einen Diebstahl eines Clientsystems oder einen Austausch gegen ein anderes Clientsystem unterstützt werden.

T.AK.Mani.TI	Angriff durch manipulierte Systeme der zentralen TI-Plattform

Ein Angreifer mit Zugriff auf Systeme in der zentralen Telematikinfrastruktur-Plattform manipuliert Systeme bzw. Fachanwendungen, mit denen der EVG kommuniziert. Dadurch werden sensible Daten wie beispielsweise Kommunikationsschlüssel (Metadaten) oder übertragene zu schützende Daten (Nutzerdaten) kompromittiert. Weiterhin können diese Systeme unautorisierten Zugriff auf den EVG über eine bestehende Datenverbindung erlangen um Zugriff auf dort gespeicherte Nutzer- und Metadaten zu erhalten.

T.AK.Mani.ExternerDienst	Angriff durch einen manipulierten externen Dienst

Ein Angreifer mit Zugriff auf Komponenten externer Dienste, wie etwa dem PKI oder Zeit-Dienst, kann diesen Dienst manipulieren oder verhindern. Damit wird der EVG mit gefälschten PKI- oder Zeit-Informationen versorgt oder die PKI- oder Zeit-Informationen werden komplett blockiert. Dadurch können Sicherheitsdienste des EVG, etwa die Prüfung von Zertifikaten, beeinflusst oder unterbunden werden.

T.AK.Mani.Chipkarte	Angriff durch manipulierte Chipkarte(n)

Ein Angreifer mit Zugriff auf eine verwendete Chipkarte manipuliert diese, um beispielsweise darauf gespeicherte Geheimnisse auszulesen oder mit dem Angreifer bekannten Daten zu überschreiben. Weiterhin kann er auf die Funktion der Karte Einfluss nehmen, um beispielsweise das Ergebnis einer Signaturprüfung zu fälschen.

T.AK.Mani.Terminal	Manipuliertes Kartenterminal

Ein Angreifer mit Zugriff auf eHealth-Kartenterminals manipuliert diese, um unautorisierten Zugang zu Geheimnissen (PIN) zu erlangen oder um sensitive Daten (etwa die Anzeige auf dem Display) zu modifizieren (Wert: Metadaten und Authentisierungsgeheimnisse bei der Bearbeitung im Kartenterminal).

T.AK.Mani.AdminKonsole	Manipulierte Administrationskonsole

Ein Angreifer manipuliert die Administrationskonsole oder setzt ein unautorisiertes System als Administrationskonsole ein. Damit wird unautorisierter Zugriff auf das EVG ermöglicht. In einem weiteren Szenario nutzt ein autorisierter Administrator die manipulierte Konsole und kann damit unbemerkt administrative Funktionen des Angreifers im EVG ausführen. Betroffen sind die Management-Daten bei Übertragung zum und Verarbeitung im EVG.

3.2.2.6. Bedrohungen in den Betriebsabläufen

T.AK.MissbrauchKarte Missbrauch von Chipkarten

Ein Angreifer kann die PIN eines autorisierten Benutzer bei der Eingabe ausspähen. Wenn später die Chipkarte gestohlen wird, kann der Angreifer die Karte unautorisiert zum Zugriff auf Funktionalität oder Daten (Nutzerdaten und Metadaten) des EVG verwenden oder sogar Daten auf der Chipkarte modifizieren.

T.AK.Fehlbedienung Datenverfälschung oder Fehlkonfiguration durch Fehlbedienung

Ein autorisierter Benutzer oder Administrator kann durch Fehlbedienung am Clientsystem bzw. an der Administrationskonsole ungewollte Systemzustände herbeiführen, die zu schützende Daten in ungewollter Weise beeinflussen können. Das kann beispielsweise ein ungewolltes Löschen von Daten bedeuten oder (im Fall des Administrators) das Aktivieren einer ungewollten Konfigurationsoption. Betroffene Werte sind die Nutzerdaten und Metadaten sowie Management-Daten.

3.3. Organisatorische Sicherheitspolitiken

3.3.1. Organisatorische Sicherheitspolitiken des Netzkonnektors

In den folgenden Tabellen werden die „Organisatorische Sicherheitspolitiken des Netzkonnektors“ wiedergegeben. Diesen wurden unverändert aus dem PP [17] übernommen.

OSP.NK.Zeitdienst Zeitdienst

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

OSP.NK.SIS Sicherer Internet Service

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

OSP.NK.BOF Kommunikation mit Bestandsnetzen und offenen Fachdiensten

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

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

Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30]. Zudem prüft der EVG die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

OSP.NK.SW-Update Software-Update

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

Es dürfen nur von einer autorisierten Stelle geprüfte, freigegebene und ggf. zertifizierte Komponenten bzw. Fachmodule signiert und zum Update bereitgestellt werden. Die Updates können je nach Konfiguration automatisch installiert werden.

Bevor ein Software-Update installiert wird, wird die Integrität und Authentizität / Zulässigkeit der Software überprüft (Signaturprüfung und Prüfung der Identität des Signierenden, Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen[17]). Schlägt die Prüfung der Integrität fehl, verhindert der EVG eine Aktualisierung der Software.

Manuelle Installationen von Updates sowie Änderungen der Konfiguration bzgl. automatischer Updates sind administrative Vörgänge und auf entsprechende Nutzer zu beschränken. Ebenso müssen Aktualisierungen Protokoliert werden.

Hinweis: OSP.AK.SW-Update und OSP.NK.SW-Update sind identisch. Die doppelte Aufführung ist historisch bedingt.

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

3.3.2. Organisatorische Sicherheitspolitiken des Anwendungskonnektors

Die organisatorischen Sicherheitspolitiken des Anwendungskonnektors ergeben sich aus gesetzlichen Anforderungen und übergreifenden Dokumenten für technische Komponenten der Telematikinfrastruktur und der elektronischen Gesundheitskarte. Die organisatorischen Sicherheitspolitiken für den Signaturdienst für die QES ergeben sich aus der eIDAS-VO [12].

3.3.2.1. allgemeine organisatorischen Sicherheitspolitiken

OSP.AK.MedSoc_Data Schutz medizinischer Daten und Sozialdaten

Der Konnektor und die eHealth-Kartenterminals schützen die Vertraulichkeit und Integrität aller Daten, die durch oder an die Telematikinfrastruktur, ein Clientsystem des Leistungserbringers sowie eine elektronische Gesundheitskarte übergeben werden, als personenbezogene medizinische Daten oder Sozialdaten. Es werden Dienste zur qualifizierten und nichtqualifizierten elektronischen Signatur, zur Chiffrierung von Dateien sowie zur kryptographischen Absicherung der Kommunikation bereitgestellt.

OSP.AK.Konn_Spez Konformität zur Spezifikation Konnektor

Der EVG erfüllt die sicherheitsrelevanten Anforderungen des Produktsteckbriefes Konnektor [28] und der Spezifikation Konnektor [27]. Der EVG stellt sichere Dienste zur Signaturerstellung, Signaturprüfung, Verschlüsselung, Entschlüsselung, Kommunikation mit den eHealth-Kartenterminals und der Verwendung der Chipkarten zur Verfügung. Ebenso bietet der EVG einen sicheren Update-Mechansimus und eine sichere Protokollierung.

Anwendungshinweis 25: Die Spezifikation Konnektor beschreibt das Verhalten des Konnektors an den äußeren Schnittstellen und Abläufe von Funktionen. Diese Sicherheitsvorgaben verweisen auf diese Beschreibungen soweit dies für die Festlegung von Sicherheitseigenschaften erforderlich ist.

OSP.AK.KryptAlgo Kryptographische Algorithmen

Alle kryptographischen Sicherheitsmechanismen der technischen Komponenten der Telematikinfrastruktur werden im Einklang mit den relevanten Vorgaben des Dokuments TR-03116-1 [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30] implementiert. Für den Signaturdienst für qualifizierte elektronische Signaturen gelten die Festlegungen gemäß [12].

OSP.AK.SW-Update Software-Update

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

Es dürfen nur von einer autorisierten Stelle geprüfte, freigegebene und ggf. zertifizierte Komponenten bzw. Fachmodule signiert und zum Update bereitgestellt werden. Die Updates können je nach Konfiguration automatisch installiert werden.

Bevor ein Software-Update installiert wird, wird die Integrität und Authentizität / Zulässigkeit der Software überprüft (Signaturprüfung und Prüfung der Identität des Signierenden, Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen[18]). Schlägt die Prüfung der Integrität fehl, verhindert der EVG eine Aktualisierung der Software.

Manuelle Installationen von Updates sowie Änderungen der Konfiguration bzgl. automatischer Updates sind administrative Vörgänge und auf entsprechende Nutzer zu beschränken. Ebenso müssen Aktualisierungen Protokoliert werden.

Hinweise: OSP.AK.SW-Update und OSP.NK.SW-Update sind identisch. Die doppelte Aufführung ist historisch bedingt. Der Konnektor unterstützt die Funktion „AutoUpdate“. Die Fachmodule sind im Image des Anwendungskonnektors enthalten. Updates für Fachhmodule oder zusätzliche Fachmodule können nur über ein Update der Konnektor-Software eingebracht werden.

3.3.2.2. Organisatorische Sicherheitspolitiken zur Signaturerzeugung und Signaturprüfung

OSP.AK.SC_Sign Erzeugung elektronischer Signaturen

Der Signaturschlüssel-Inhaber nutzt den Heilberufsausweis als qualifizierte Signaturerstellungseinheit sowie den EVG und die eHealth-Kartenterminals mit gSMC-KT zur Erstellung qualifizierter elektronischer Signaturen. Der Benutzer kann den EVG auch zur Erzeugung nicht-qualifizierter elektronischer Signaturen für Dokumente nutzen. Der EVG stellt Schnittstellen für die Erzeugung digitaler (nicht.qualifizierter) Signaturen über Bitstrings mit Authentisierungsschlüsseln bereit.

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

OSP.AK.SC_Authorized Autorisierung der Signatur

Bei der Erzeugung einer qualifizierten elektronischen Signatur muss durch den Signaturdienst gewährleistet sein, dass eine Signatur nur durch die berechtigt signierende Person erfolgt.

OSP.AK.SC_SVAD Schutz der Authentisierungsdaten

Bei der Erzeugung einer qualifizierten elektronischen Signatur muss durch den Signaturdienst gewährleistet sein, dass die Authentisierungsdaten nicht preisgegeben und diese nur auf der jeweiligen qualifizierten Signaturerstellungseinheit gespeichert werden.

OSP.AK.SC_UnalteredData Unversehrtheit der zu signierenden Daten

Der Prozess der Erstellung von Signaturen ist auf Abweichungen zu überwachen und der Benutzer ist über festgestellte Abweichungen zu informieren. Die Erzeugung qualifizierter elektronischer Signaturen darf nur für die vom Signaturschlüssel-Inhaber übergebenen Daten erfolgen, bei festgestellten Abweichungen sind alle Signaturen des Stapels zu verwerfen.

OSP.AK.SV_Certificate Prüfung des Zertifikates

Bei der Verifizierung einer qualifizierten elektronischen Signatur muss durch den EVG geprüft werden, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Für die Prüfung nicht-qualifizierter elektronischer Signaturen und digitaler Signaturen können gesonderte Regeln in der Signaturrichtlinie der signierten Daten festgelegt werden.

OSP.AK.SV_Signatory Zuordnung des Signaturschlüssel-Inhabers

Für die Überprüfung qualifiziert signierter Daten sind Komponenten erforderlich, die feststellen lassen, „welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist“. Die Prüfung nicht-qualifizierter elektronischer Signaturen und digitaler Signaturen muss den Signaturschlüssel-Inhaber, dem die Signatur zuzuordnen ist, feststellen lassen.

OSP.AK.SV_Unaltered_Data Unversehrtheit der signierten Daten

Der EVG muss bei der Überprüfung qualifiziert signierter Daten gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird und insbesondere, ob die signierten Daten unverändert sind. Die Prüfung nicht-qualifizierter elektronischer Signaturen und digitaler

Signaturen muss feststellen lassen, ob die signierten Daten unverändert sind und welche Prüfungsergebnisse dafür vorliegen.

OSP.AK.EVG_Modification	Schutz vor Veränderungen

Sicherheitstechnische Veränderungen an der EVG-Komponente für qualifizierte elektronische Signaturen müssen für den Nutzer erkennbar werden. Dauerhaft gespeicherte Klartextschlüssel sind gegen Kompromittierung durch physische und logische Angriffe zu schützen.

3.3.2.3. Organisatorische Sicherheitspolitiken für Kryptomodul und Server

OSP.AK.Encryption	Verschlüsselung und Entschlüsselung

Der Konnektor muss Dienste zum Verschlüsseln und Entschlüsseln von Daten im Rahmen fachlicher Anwendungsfälle bereitstellen. Dem Konnektor werden durch das Clientsystem die zu verschlüsselnden und zu entschlüsselnden Dokumente übergeben, die zu verwendende Verschlüsselungsrichtlinie durch den Fachdienst bzw. den Anwendungsfall identifiziert und beim Verschlüsseln eines Dokuments die vorgeschlagenen Empfänger des Dokuments angegeben. Vor dem Verschlüsseln eines Dokuments wird die Gültigkeit der zu benutzenden Verschlüsselungszertifikate geprüft. Alle Verschlüsselungsrichtlinien, die vom Konnektor umgesetzt werden, erlauben das automatische Verschlüsseln und Entschlüsseln von Daten.

OSP.AK.CardService	Chipkartendienste

Der EVG muss Sicherheitsdienste zur lokalen und entfernten Eingabe von PIN und PUK, zur Identifizierung und Authentisierung von Chipkarten sowie zur gegenseitigen Authentisierung zwischen Chipkarten (Card-to-Card-Authentisierung) in den angeschlossenen eHealth-Kartenterminals erbringen. Der EVG kontrolliert den Zugriff auf Chipkarten in Abhängigkeit von deren Sicherheitszustand.

3.3.2.4. Organisatorische Sicherheitspolitiken für Fachanwendungen

OSP.AK.Fachanwendungen	vertrauenswürdige Fachanwendungen und zentrale Dienste der TI-Plattform

Die Fachanwendungen der TI und zentrale Dienste der TI-Plattform sind vertrauenswürdig und verhalten sich entsprechend ihrer Spezifikation. Der Konnektor unterstützt den Fachdienst Versichertenstammdatenmanagement und die Kommunikation mit dem zentralen Verzeichnisdienst. Fachdienste und Fachmodule kommunizieren über gesicherte Kanäle. Für zentrale Dienste der TI kann eine geschützte Kommunikation bereit gestellt werden. Durch

Fachanwendungen genutztes Schlüsselmaterial wird wirksam vor Angriffen geschützt. Wird dennoch eine Komponente einer Fachanwendung und/oder sein Schlüsselmaterial erfolgreich angegriffen, so werden die betroffenen Schlüssel zeitnah gesperrt.

3.3.2.5. Organisatorische Sicherheitspolitiken für die ePA Fachanwendung (PTV4)

OSP.AK.VAUSGD	Geschützte Kommunikation mit VAU-Instanz und SGD-HSM

Der Konnektor muss das „VAU-Protokoll“ zur Kommunikation mit der VAU-Instanz in der ePA-Dokumentenverwaltung und das „SGD-Protokoll“ zur Kommunikation mit dem SGD-HSM des Schlüsselgenerierungsdienst spezifikationskonform umsetzen, um den Wert VAU-/SGD-Inhaltsdaten zu schützen. Die korrekte Implementierung der Protokolle sichert den Datenverkehr des TOE mit der VAU-Instanz in der ePA-Dokumentenverwaltung und dem SGD-HSM des Schlüsselgenerierungsdienst gegen unbefugtes Mithören ab. Die korrekte Implementierung schützt nicht gegen einen aktiven Angreifer, der einen einzelnen Konnektor zu manipulieren versucht.

3.4. Annahmen

3.4.1. Annahmen an den Netzkonnektor

In den folgenden Tabellen werden die „Annahmen an den Netzkonnektor“ wiedergegeben. Diesen wurden unverändert aus dem PP [17] übernommen.

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

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

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

Hinweis: Die Annahme A.NK.phys_Schutz an den Netzkonnektor ist identisch zur Annahme A.AK.phys_Schutz an den Anwendungskonnektors. Der Konnektor wird als Einbox-Konnektor umgesetzt.

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

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

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

Die gSMC-K ist durch die gematik zugelassen.

Anwendungshinweis 26: Nicht relevant. In der Konnektor-Hardware werden physische gSMC-Ks verbaut

A.NK.sichere_TI	Sichere Telematikinfrastruktur-Plattform

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

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

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

Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

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

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

Anwendungshinweis 27: Der Beitrag des EVG zur Abwehr von Denial of Service Angriffen besteht lediglich darin, dass nur autorisierten Benutzern Zugang zu den Diensten der Telematikinfrastruktur vermittelt wird. Zudem trägt die Verwendung von DNSSEC bei der Ermittlung von IP-Adressen der VPN Konzentratoren TI und SIS zur Abwehr von DoS Angriffen bei. Insofern kann der Netzkonnektor die Abwehr von Denial of Service Angriffen unterstützen, aber nicht die alleinige Verantwortung dafür übernehmen. Die Verantwortung für den Schutz der Systeme der zentralen Telematikinfrastruktur-Plattform liegt bei den Firewall-Systemen im Perimeter der zentralen Telematikinfrastruktur-Plattform. Der Schwerpunkt der Abwehr durch den EVG liegt bei den in O.NK.PF_WAN und O.NK.PF_LAN beschriebenen Bedrohungen.

A.NK.AK	Anwendungskonnektor nutzt EVG korrekt

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

Anwendungshinweis 28: Der EVG implementiert einen Paketfilter und stellt separate Kommunikationskanäle für Daten, welche zu schützende Daten der TI und der Bestandsnetze sind (z. B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur-Plattform) und entsprechend gekennzeichnet sind zur Verfügung. Basierend auf der Informationsflusskontrolle wertet der Paketfilter die IP Information aus, welche über die logischen Schnittstellen ausgetauscht wird.

A.NK.CS	Clientsystem nutzt EVG korrekt

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

Anwendungshinweis 29: Der EVG implementiert einen Paketfilter und stellt separate Kommunikationskanäle für Daten, welche zu schützende Daten der TI *und der Bestandsnetze* sind (z. B. personenbezogene medizinische Daten für die zentrale Telematikinfrastruktur-Plattform) und entsprechend gekennzeichnet sind zur Verfügung. Basierend auf der Informationsflusskontrolle wertet der Paketfilter die IP Information aus, welche über die logischen Schnittstellen ausgetauscht wird.

A.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

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

Er setzt nur gemäß dem Schutzprofil [16] zertifizierte Anwendungskonnektoren ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.

Er administriert die Anwendungskonnektoren in sicherer Art und Weise.

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

A.NK.Betrieb_CS Sicherer Betrieb der Clientsysteme

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

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

Er administriert die Clientsysteme in sicherer Art und Weise.

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

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

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

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

A.NK.Admin_EVG Sichere Administration des EVG

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

Personal einzusetzen. Die Administratoren halten Authentisierungsinformationen und –token geheim bzw. geben diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token).

A.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

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

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

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

Anwendungshinweis 30: Dieser Aspekt wird im Schutzprofil [16] als übergreifende Sicherheitsfunktion modelliert.

3.4.2. Annahmen an den Anwendungskonnektor

In den folgenden Tabellen werden die „Annahmen an den Anwendungskonnektor“wiedergegeben. Diesen wurden unverändert aus dem PP [17] übernommen.

A.AK.Versicherter Sorgfaltspflichten des Versicherten

Der Versicherte händigt seine eGK nur dann und nur dort einem HBA-Inhaber oder einem seiner Mitarbeiter aus, wenn er diesem Zugriff auf seine Daten gewähren will. Er nimmt seine eGK nach Abschluss der Konsultation wieder an sich.

A.AK.HBA-Inhaber Vertrauenswürdigkeit und Sorgfaltspflichten des HBA-Inhabers

Der HBA-Inhaber und seine Mitarbeiter sind vertrauenswürdig in Bezug auf den Umgang mit den ihm bzw. ihnen anvertrauten zu schützenden Daten. Alle Leistungserbringer, die Zugriff auf medizinische Daten haben, welche auf Clientsystemen lokal gespeichert werden, gehen verantwortungsvoll mit diesen Daten um.

Der Betreiber des Konnektors administriert seine IT-Umgebung in einer Art und Weise, die Missbrauchsmöglichkeiten minimiert. Der HBA-Inhaber verwendet seinen HBA nur in IT-Umgebungen, die wie im vorigen Satz beschrieben sicher administriert werden.

A.AK.SMC-B-PIN Freischaltung der SMC-B

Die SMC-B ist nur freigeschaltet, wenn sie und der Konnektor unter der Kontrolle des Leistungserbringers arbeiten. Wenn der Leistungserbringer keine Kontrolle mehr über den Konnektor oder die SMC-B hat, setzt er die Freischaltung der SMC-B zurück (z.B. durch Ausschalten des Kartenterminals oder Ziehen der Chipkarte).

A.AK.sichere_TI Sichere Telematikinfrastruktur-Plattform

Die zentrale Telematikinfrastruktur-Plattform wird als vertrauenswürdig angesehen, d.h., Angriffe aus der zentralen Telematikinfrastruktur-Plattform werden nicht betrachtet und es wird angenommen, dass die zentrale Telematikinfrastruktur-Plattform die ihr anvertrauten Daten / Informationen nicht missbraucht. Die Administration der Telematikinfrastruktur sorgt dafür, dass die Server in der Telematikinfrastruktur frei von Schadsoftware gehalten werden, so dass über bestehende logische Kanäle zum AK keine Angriffe auf den AK erfolgen. Alle Administratoren der Telematikinfrastruktur sind fachkundig und vertrauens-würdig

A.AK.Admin_EVG Sichere Administration des Anwendungskonnektors

Der Betreiber des AKs sorgt dafür, dass administrative Tätigkeiten in Übereinstimmung mit der Administrator-Dokumentation des AKs durchgeführt werden. Insbesondere wird für diese Tätigkeiten vertrauenswürdiges und hinreichend geschultes Personal eingesetzt. Der Administrator handelt nur im Sinne des verantwortlichen Leistungserbringers bzw. Konnektor-Betreibers und in dessen Auftrag. Der Administrator ist verantwortlich dafür die automatische Aktualisierung des Konnektor zu konfigurieren und hat im Falle des manuellen Anwendens von Aktualisierungen das Recht das Update anzustoßen. Der Administrator hält Authentisierungsinformationen und -token geheim bzw. gibt diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token). Der Leistungserbringer als Nutzer des Konnektors hat die Verantwortung, die Eignung der aktuell genutzten Konnektorfirmware-Version zu prüfen.

Anwendungshinweis 31: Die Information der Benutzer des AKs, welche Firmware-Version aktuell genutzt wird kann vom Administrator über die Managementschnittstelle ausgelesen werden. Der Konnektor unterstützt die automatische Aktualisierung („AutoUpdate“). Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartenterminals organisatorisch genschützt werden.

A.AK.Cardterminal_eHealth	Nutzung eines sicheren Kartenterminals

Für die Chipkarten und die Eingabe von Benutzerverifikationsdaten werden ausschließlich eHealth-Kartenterminals verwendet, die der Spezifikation [38] entsprechen und nach dem Schutzprofil für eHealth-Kartenterminals [22] evaluiert wurden.

A.AK.Konnektor	Konnektor

Die Anwender/Benutzer setzen nur solche Konnektoren ein, welche der Spezifikation [27] entsprechen und nach dem Konnektor Schutzprofil BSI-CC-PP-0098 evaluiert und zertifiziert wurden. Die Plattform des Konnektors stellt dem EVG eine Ausführungsumgebung zur Verfügung, die die von ihm verarbeiteten Daten vor dem Zugriff durch Dritte (andere Programme, Prozesse, IT-Systeme o. ä.) schützt.

A.AK.Env_Arbeitsplatz	Vertrauenswürdige Einsatzumgebung

Der Arbeitsplatz des Clientsystems ist vertrauenswürdig. Wenn dem Benutzer des EVGs zu signierende Daten oder Prüfergebnisse auf dem Arbeitsplatz des Clientsystems angezeigt werden, so wird die genutzte Anzeigekomponente ebenfalls als vertrauenswürdig angesehen.

A.AK.Benutzer_Signatur	Prüfung zu signierender und zu prüfender Dokumente vor der Übermittlung an den AK

Der Benutzer des Clientsystems sorgt vor der Übermittlung an den AK dafür, dass er nur solche Daten zur Signaturerzeugung und zur Signaturprüfung über sein Clientsystem an den AK übergibt, welche er auch tatsächlich signieren bzw. verifizieren will.

A.AK.SMC	Nutzung einer SMC-B und gSMC-KT

Es werden nur solche Chipkarten mit privaten Schlüsseln und dazu gehörigen CVC als SMC-B bzw. gSMC-KT ausgestattet und in den eHealth-Kartenterminals betrieben, deren Betriebssystem der Spezifikation [31] entspricht und nach dem Schutzprofil COS Schutzprofil [15] evaluiert ist und dessen Objektsysteme der Spezifikation [36] bzw. [34] entsprechen.

Die genutzte SMC hat eine TR-Zertifizierung nach BSI TR-03144 erfolgreich durchlaufen (Nachweis der vertrauenswürdigen Initialisierung) und die Personalisierung der SMC ist sicher.

Der Chipkartentyp SMC kann aus verschiedenen Quellen auf der jeweiligen Karte verlässlich bestimmt werden (bspw. CV-Zertifikat und X.509-Zertifikat). Bei der Personalisierung der

SMC wird sichergestellt, dass die Konsistenz hinsichtlich des Kartentyps zwischen diesen Quellen gewahrt ist.

A.AK.gSMC-K	Nutzung einer gSMC-K

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

Die gSMC-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des EVG repräsentiert und von ihm verwendet wird. Es führt kryptographische Operationen mit diesem Schlüsselmaterial durch, ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.

Die gSMC-K ist durch die gematik zugelassen.

Die genutzte gSMC-K hat eine TR-Zertifizierung nach BSI TR-03144 erfolgreich durchlaufen (Nachweis der vertrauenswürdigen Initialisierung) und die Personalisierung der gSMC-K ist sicher.

A.AK.QSCD	Nutzung einer qualifizierten Signaturerstellungseinheit

Es werden nur solche Chipkarten mit privaten Schlüsseln und dazu gehörigen CVC als HBA ausgestattet, deren Betriebssystem der Spezifikation [31] entspricht und nach dem Schutzprofil COS [15] evaluiert ist, deren Objektsysteme der Spezifikation [35] entspricht und das als qualifizierte elektronische Signaturerstellungseinheit nach eIDAS zertifiziert ist.

Anwendungshinweis 32: Gemäß Spezifikation [35] wird der Heilberufsausweis mit einem privaten Signaturschlüssel ausgestattet, zu dessen öffentlichen Prüfschlüssel ein zum Zeitpunkt der Ausgabe gültiges qualifiziertes Zertifikat existiert. Der AK prüft für die Erzeugung qualifizierter elektronischer Signaturen, ob dieses Zertifikat zu dem Signaturzeitpunkt oder - wenn dieser nicht bekannt ist – einem angegebenen Zeitpunkt der Signatur gültig ist. Insbesondere erzwingt der HBA, dass für eine Stapelsignatur und auch für eine Komfortsignatur sowohl eine erfolgreiche Authentisierung mit der QES.PIN erfolgt als auch die zu signierenden Daten mit Secure Messaging übersendet werden, das auf der Basis einer Authentisierung der Gegenstelle mit der Identität „SAK“ gebildet wurde.

A.AK.Chipkarteninhaber	Vertrauenswürdigkeit und Sorgfaltspflichten des Chipkarteninhabers

Der Chipkarteninhaber ist vertrauenswürdig in Bezug auf den Umgang mit den ihm anvertrauten zu schützenden Daten. Der Chipkarteninhaber des HBA und der SMC-B wendet seine Chipkarte nur in Umgebungen an, in denen der Leistungserbringer sicherstellt, dass die

IT-Umgebung des Leistungserbringers (insbesondere das Clientsystem) vertrauenswürdig ist.

Der Chipkarteninhaber darf seine PIN.CH nur dann an einem Kartenterminal eingeben, wenn der durch den Chipkarteninhaber initiierte Anwendungsfall dies erfordert und wenn das Kartenterminal dem Chipkarteninhaber einen sicheren PIN-Eingabemodus anzeigt. Wird der Chipkarteninhaber von einem Kartenterminal zur PIN-Eingabe aufgefordert, ohne dass das Kartenterminal gleichzeitig den sicheren PIN-Eingabemodus anzeigt, muss der Chipkarteninhaber den Vorgang abbrechen und darf seine PIN nicht eingeben.

Der Chipkarteninhaber des HBA und der SMC-B kontrolliert bei der entfernten PIN-Eingabe die Übereinstimmung der Jobnummer, die ihm auf dem Clientsystem anzeigt wird mit der Anzeige auf dem PIN-Kartenterminal. Bei nicht übereinstimmender Jobnummer bricht der Chipkarteninhaber den Vorgang ab.

A.AK.phys_Schutz Physischer Schutz des Konnektors

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

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

Hinweis: Die Annahme A.AK.phys_Schutz an den Anwendungskonnektor ist identisch zur Annahme A.NK.phys_Schutz an den Netzkonnektors. Der Konnektor wird als Einbox-Konnektor Umgesetzt.

4. Sicherheitsziele

Die Namensgebung der symbolischnen Bezeichner für die im Folgenden definierten Sicherheitsziele folgt der aus dem zugrundeliegenden dem PP [16].

4.1. Sicherheitsziele für den Netzkonnektor

In den folgenden Tabellen werden die „Sicherheitsziele für den Netzkonnektor“ wiedergegeben. Diesen wurden unverändert aus dem PP [16] übernommen und um die Sicherheitsziele O.NK.Update und O.NK.Admin_Auth erweitert.

4.1.1. Allgemeine Ziele: Schutz und Administration

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

Der NK stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30]. Zudem prüft der NK die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

Anwendungshinweis 33: Für welche Verbindungen TLS-Kanäle genutzt werden, ist Gegenstand des Anwendungskonnektors. Der Netzkonnektor stellt die kryptographische Grundfunktionalität für TLS zur Verfügung.

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

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

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

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

Anwendungshinweis 34: **Annahmen zum physischen Schutz**: Der Schutz vor physischen Angriffen wird durch die Einsatzumgebung gewährleistet (siehe A.NK.phys_Schutz). Der EVG schützt die TSF Daten (den ausführbaren Code) auf der Basis von geeigneten kryptographischen Signaturen unter Nutzung von Vorgaben gemäß TR-03116-1 [19].

O.NK.EVG_Authenticity Authentizität des EVG

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

Anwendungshinweis 35: Die Auslieferung des Netzkonnektor gegenüber dem empfangenden Leistungserbringer oder dem von ihm beauftragten Servicetechniker erfolgt durch gesicherten Transport. Nach Erhalt des Netzkonnektors muss dieser bis zur Inbetriebnahme in einem gesicherten Bereich aufbewahrt werden. Der Betrieb selbst findet in einer sicheren Umgebung statt (siehe OE.NK.phys_Schutz). Die Authentizität des EVG wird dadurch nachgewiesen, dass der Netzkonnektor sich erfolgreich gegenüber einem VPN-Konzentrator für Dienste gemäß § 291 a SGB V [14] authentisiert hat und fachliche Anwendungsfälle im Online-Modus durchgeführt werden können.

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

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

Dazu ermöglicht der NK die sichere Identifikation und Autorisierung eines Administrators, welcher die lokale und entfernte Administration des EVG durchführen kann. Der Anwendungskonnektor stellt nur authorisierten Administratoren die Management Funktionen des NK zur Verfügung.

Die Administration erfolgt über Netzverbindungen (lokal über PS2 oder zentral über PS3). Die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen wird durch eine TLS Verbindung abgesichert (Administration über einen sicheren logischen Kanal).

Der NK **verhindert** die Administration folgender Firewall-Regeln:

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

- Regeln für die Kommunikation zwischen LAN und den Bestandsnetzen (außer Freischalten aktiver Bestandsnetze),

Anwendungshinweis 36: Der EVG unterstützt die Rolle Administrator. Dabei werden im EVG die Administrator-Rollen local administrator, remote administrator und super administrator unterschieden. Der lokale und Remote Administrator können den EVG jeweils über einen entsprechenden Port an der LAN-Schnittstelle konfigurieren. Der Super Administrator benutzt die gleiche Schnittstelle wie der lokale Administrator und kann zudem Benutzerkonten verwalten und Zugriffsrechten vergeben. Es können alle Management-Funktionen der TSF von den drei Administratoren (mit den entsprechenden Einschränkungen nach TAB_KON_655 und TAB_KON_851 aus [27] für den remote administrator) ausgeführt werden. Daher werden unter dem Subjekt Administrator in den SFRs die einzelnen Rollen zusammengefasst.

Anwendungshinweis 37: Jede Änderung, die ein Administrator vornimmt, wird zusammen mit einem Zeitstempel und der Identität (Identifikator) des Administrators protokolliert.

Anwendungshinweis 38: Der für die Administration notwendige sichere logische Kanal muss auf den durch [26] vorgegebenen Protokollen und Algorithmen beruhen.

O.NK.Protokoll Protokollierung mit Zeitstempel

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

Anwendungshinweis 39: Der für das Protokoll erforderliche Zeitstempel wird dabei durch O.NK.Zeitdienst bereitgestellt.

Anwendungshinweis 40: Eine Protokollierung von Zugriffen auf medizinische Daten nach § 291 a (6) Satz 2 SGB V erfolgt durch den Anwendungskonnektor (auf der eGK oder in der zentralen Telematikinfrastruktur-Plattform). Diese Art der Protokollierung ist hier nicht gemeint; der EVG ist in die Protokollierung von Zugriffen auf medizinische Daten nicht involviert.

O.NK.Zeitdienst Zeitdienst

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

Anwendungshinweis 41: Die sichere Systemzeit wird u. a. für die Gültigkeitsprüfung von Zertifikaten von VPN-Konzentratoren verwendet.

O.NK.Update	Software Update

Bevor Updatedaten für den NK oder andere Komponenten bereitgestellt werden, muss die Integrität und die Authentizität / Zulässigkeit der Updatedaten überprüft (Signaturprüfung und Prüfung der Identität des Signierenden) und Metadaten (zum Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen) angezeigt werden. Schlägt die Prüfung der Integrität fehl, verhindert der NK die Bereitstellung der Updatedaten. Die Installation dieser Updates kann durch den Administrator oder, wenn dies vom Administrator explizit so konfiguriert wurde, automatisch erfolgen.

Hinweis: O.NK.Update wurde von O.AK.Update aus dem Protection Profile BSI-CC-PP-0098 [16] des Gesamtkonnektors abgeleitet. Der hier beschriebene Update-Vorgang für die Software des EVG bezieht sich auf die Software des Konnektors, die Updatefunktion für Software wird durch den Netzkonnektor und den Anwendungskonnektor implementiert. Die Updatefunktion für Software kann auch für das Nachladen von geprüften und freigegebenen Fachmodulen verwendet werden.

O.NK.Admin_Auth	Authentisierung des Administrators

Der NK führt selbst die Authentisierung des Administrators durch.

Hinweis: Das Sicherheitsziel OE.NK.Admin_Auth für die Umgebung aus dem zugrundeliegendem Protection Profile [16] wurde in ein Sicherheitsziel O.NK.Admin_Auth für den EVG umgewandelt, siehe auch Anwendungshinweis 53:

4.1.2. Ziele für die VPN-Funktionalität

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

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

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

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

Außerdem überprüft der EVG, dass die verwendeten Algorithmen gemäß *Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte für der* Bundesregierung, Teil 1: Telematikinfrastruktur [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30] noch gültig sind.

Anwendungshinweis 42: Der EVG implementiert die Algorithmen TR-03116-1 [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30]. Eine Prüfung der Gültigkeit der Algorithmen wird nicht explizit durchgeführt. Dies wird implizit im Rahmen der Evaluierung des Netzkonnektors sichergestellt. Weiterhin bietet der EVG keine Funktionalität die Verfügbarkeit der in Bezug auf die beannnten Spezifikationen ungültigen Algorithmen selektiv einzuschränken. Eine Einschränkung der im Konnektor verwendbaren Algortihmen kann nur über ein Software-Update erreicht werden.

O.NK.Zert_Prüf Gültigkeitsprüfung für VPN-Zertifikate

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

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

Der NK schützt die Vertraulichkeit der Nutzdaten[19] bei der Übertragung von und zu den VPN-Konzentratoren.

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

Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.

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

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

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

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

4.1.3. Ziele für die Paketfilter-Funktionalität

O.NK.PF_WAN	Dynamischer Paketfilter zum WAN

Der NK schützt sich selbst und andere Konnektorteile vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN). Wenn der Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt[20], dann schützt der NK auch die Clientsysteme.

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

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

Anwendungshinweis 43: Die Inhalte der Kommunikation über den VPN-Tunnel werden vom Konnektor nicht ausgewertet.

O.NK.PF_LAN	Dynamischer Paketfilter zum LAN

Der NK schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN

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

Anwendungshinweis 44: Siehe auch OE.NK.AK.

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

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

[20] Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [27], Kapitel 2.7.

4.2. Sicherheitsziele für den Anwendungskonnektor

Über die in Abschnitt 4.1 aufgeführten Sicherheitsziele für den Netzkonnektor hinaus werden die folgenden Sicherheitsziele für den Anwendungskonnektor definiert:

4.2.1. Allgemeine Sicherheitsziele

O.AK.Basis_Krypto Kryptographische Algorithmen

Der AK verwendet sichere kryptographische Algorithmen und Protokolle für die qualifizierte elektronische Signatur gemäß [12] und für alle anderen Kryptoverfahren des AK gemäß [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30].

O.AK.Admin Administration

Der AK erlaubt die Durchführung administrativer Funktionen nur besonders berechtigten Benutzern nach erfolgreicher Authentisierung. Dies betrifft insbesondere das Management der eHealth-Kartenterminals, Einrichten des sicheren Datenspeichers, der Arbeitsplätze und die Aktivierung und Deaktivierung der Online Kommunikation, des Signaturdienstes und der Logischen Separation sowie das Management der Konfigurationsdaten der Fachmodule. Die Administration erfolgt über eine Managementschnittstelle. Der AK erzwingt die bezüglich Vertraulichkeit und Integrität geschützte Kommunikation zur Administration über die Managementschnittstelle.

O.AK.EVG_Modifikation Schutz vor Veränderungen

Der AK macht dem Nutzer zur Laufzeit sicherheitstechnische Veränderungen erkennbar. Dauerhaft gespeicherte geheime kryptographische Schlüssel sind vor Kompromittierung durch logische Angriffe zu schützen.

O.AK.Selbsttest Selbsttests

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

O.AK.Protokoll Sicherheitsprotokoll mit Zeitstempel

Der AK protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit. Diese Protokollierung ist nicht abschaltbar. Der AK stellt sicher, dass das Sicherheitsprotokoll weder von außen noch durch den Administrator verändert oder gelöscht werden kann.

O.AK.Zeit	Systemzeit

Der AK verwendet bei sicherheitsrelevanten Aktionen (etwa das Sicherheitsprotokoll, siehe O.AK.Protokoll) eine sichere Systemzeit. Dabei greift er auf die Echtzeituhr zurück (siehe OE.AK.Echtzeituhr), die in regelmäßigen Abständen vom Netzkonnektor mit einem vertrauenswürdigen Zeitdienst synchronisiert ist (siehe O.NK.Zeitdienst).

O.AK.Infomodell	Umsetzung des Informationsmodells durch den AK

Der AK verwaltet die persistente Zuordnung von Mandanten, Clientsystemen, Arbeitsplätzen und Kartenterminals sowie die transiente Zuordnung von Benutzern der Arbeitsplätze, in Kartenterminals gesteckten Chipkarten und Kartensitzungen zur Durchsetzung einer Zugriffskontrolle über die den Mandanten zugeordneten Ressourcen, die Chipkarten der Benutzer der Arbeitsplätze und die Chipkarten in Übereinstimmung der für die Kartensitzung erreichten Sicherheitszustände.

Anwendungshinweis 45: Das Informationsmodell des Konnektors ist in der Spezifikation [27], Kapitel 4.1.1.1 (PIC_Kon_100, Tab_Kon_507 bis Tab_Kon_510) beschrieben, Details sind dort zu entnehmen.

O.AK.Update	Software Update und Update von TSL, CRL und BnetzA-VL

Bevor Updatedaten für den EVG oder andere Komponenten bereitgestellt werden, muss die Integrität und die Authentizität / Zulässigkeit der Updatedaten überprüft (Signaturprüfung und Prüfung der Identität des Signierenden) und Metadaten (zum Schutz gegen unbefugtes Wiedereinspielen veralteter Software-Versionen) angezeigt werden. Schlägt die Prüfung der Integrität fehl, verhindert der EVG die Bereitstellung der Updatedaten. Die Installation dieser Updates kann, je nach Konfiguration automatisch oder im manuellen Fall durch den Administrator erfolgen. Wenn der Konnektor die Update-Daten (Firmware-Update-Paket) über den KSR (Update-Server) bezieht, wird dazu ein sicherer Kanal zum KSR aufgebaut.

Der AK bezieht die Trust-service Status List (TSL) und die Certificate Revocation List (CRL). Er bezieht ebenfalls die Vertrauensliste der Bundesnetzagentur (BNetzA-VL) über den TSL-Dienst, sofern diese in einer aktualisierten Version verfügbar ist. Der für die Aktualitätsprüfung vom TSL-Dienst bezogene Hash-Wert der BNetzA-VL muss auf dem Transportweg geschützt werden.

Im Fall der erfolgreichen Prüfung der Integrität und Authentizität der genannten Listen wird der interne Speicher des EVG mit den Inhalten der bezogenen Listen aktualisiert.

Der beschriebene Update-Vorgang für die Software des EVG bezieht explizit die Software des Netzkonnektors mit ein. Es steht dem Autor der Sicherheitsvorgaben frei, die Updatefunktion für Software komplett oder in Teilen durch den Netzkonnektor zu

implementieren. In diesem Fall ist dieses Sicherheitsziel und die entsprechenden Sicherheitsanforderungen anzupassen und in den Sicherheitsvorgaben des Netzkonnektors zu berücksichtigen. Weiterhin steht es dem Autor der Sicherheitsvorgaben frei, die Updatefunktion für Software auch für das Nachladen von geprüften und freigegebenen Fachmodulen zu verwenden.

Hinweis: Das Sicherheitsziel O.AK.Update wurde unverändert aus dem zugrundeliegenden PP [16] übernommen. Die Freiheitsgrade des ST-Autors im letzten Absatz sind wie folgt umgesetzt: Die Updatefunktion für Software wird zusammen von Anwendungskonnektor und Netzkonnektor umgesetzt. Die Sicherheitsanforderungen zum Netzkonnektor wurden entsprechend angepasst. Die Updatefunktion kann indirekt zum Nachladen von geprüften und freigegebenen Fachmodulen verwendet werden. Dabei ist aber immer ein komplettes Software Update durchzuführen in dem entsprechende Fachmodule enthalten sind. Eine Funktion zum separaten nachladen von Fachmodulen, unabhängig vom Software Update des EVGs ist nicht implementiert.

4.2.2. Signaturdienst

O.AK.Sig.SignQES Signaturrichtlinie für qualifizierte elektronische Signaturen

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen für Dokumente in den Formaten Text, PDF/A, TIFF und XML[21]. Die Wohlgeformtheit der zu signierenden Dokumente wird gegen die entsprechende Format-Spezifikation geprüft. Bei reinen Textdokumenten (UTF-8 oder ISO-8859-15), PDF/A und TIFF wird die komplette Datei signiert. Die Signaturformate sind für XML, PDF/A, Text und TIFF das CadES [85] [88] sowie zusätzlich für PDF/A gemäß PAdES [86] [89] und für XML zusätzlich XAdES [82] [87]. Schlägt die Prüfung der Authentizität dieser TSF-Daten, die Prüfung der Wohlgeformtheit der zu signierenden Dokumente fehl oder kann nicht durchgeführt werden, wird dem Clientsystem über die Schnittstellen eine entsprechende Warnung ausgegeben.

Anwendungshinweis 46: Die Signaturrichtlinie bestimmt, welche Daten durch den Signaturschlüsselinhaber signiert werden. Sie kann, z. B. im Fall von XML-Signaturen neben der Signaturerzeugung und der Signaturprüfung auch für die weitere automatische Verarbeitung des Dokumentes, beispielsweise für Fachanwendungen, genutzt werden. Deshalb sind die Regeln für die QES und die Verarbeitung aufeinander abzustimmen, um z. B. XML-Signature-Wrapping-Angriffe zu verhindern. Qualifizierte XAdES Signaturen werden ausschließlich unter Verwendung einer im Konnektor enthaltenen oder von Fachmodulen übergebenen Signaturrichtlinie erstellt und geprüft.

Anmerkung 4. Nach O.AK.Sig.SignQES wird die Wohlgeformtheit der zu signierenden Dokumente gegen die entsprechende Format-Spezifikation geprüft. Das beinhaltet insbesondere die Prüfung gegen das in der NFDM-Signaturrichtline festgelegte XML Schema.

[21] Dies entspricht dem Stand der Liste unterstützter Formate zum Zeitpunkt der Erstellung des ST.

O.AK.Sig.SignNonQES Signaturrichtlinie für nichtqualifizierte elektronische Signaturen

Der AK erlaubt die Erzeugung von digitalen Signaturen für nicht-qualifizierte elektronische Signaturen für Dokumente in den Formaten Text, PDF/A, TIFF und von binären Dokumente sowie für Binärstrings[22]. Die Wohlgeformtheit der zu signierenden Dokumente wird (außer für Binärdokumente) gegen die entsprechende Format-Spezifikation geprüft. Schlägt diese Prüfung der Wohlgeformtheit der zu signierenden Dokumente fehl oder kann nicht durchgeführt werden, wird eine entsprechende Fehlermeldung erzeugt.

O.AK.Sig.exklusivZugriff Unterstützung bei alleiniger Kontrolle

Der AK stellt Methoden zur Verfügung, die es dem Signaturschlüssel-Inhaber ermöglichen, die alleinige Kontrolle über die QSEE auszuüben. Der AK initiiert die Erzeugung qualifizierter elektronischer Signaturen nur für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten.

Der AK überwacht die Integrität der zum Signieren vom AK übergebenen Daten. Der AK überprüft, ob für die vom autorisierten Benutzer übergebenen Daten ordnungsgemäße qualifizierte elektronische Signaturen erstellt wurden.

O.AK.Sig.Einfachsignatur Einfachsignatur

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen durch eine Einfachsignatur gemäß [21] mit lokaler oder entfernter PIN-Eingabe. Der AK setzt die Authentisierung des Inhabers des HBAx mittels Eingabe der QES-PIN durch. Der AK steuert die Eingabe der QES-PIN am eHealth-Kartenterminal und die Erzeugung der digitalen Signatur durch den HBA für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten. Bei festgestellten Abweichungen im Signaturprozess wird der Benutzer informiert und die erzeugte Signatur verworfen.

O.AK.Sig.Stapelsignatur Stapelsignatur

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen durch eine Stapelsignatur gemäß [21]. Der AK steuert die lokale oder entfernte Eingabe der QES-PIN am eHealth Kartenterminal und die Erzeugung der digitalen Signaturen durch den HBA. Der AK authentisiert sich gegenüber dem HBA mit der Identität „SAK“. Die Kommunikation zwischen AK und HBA ist per Secure Messaging geschützt.

[22] Dies entspricht dem Stand der Liste unterstützter Formate zum Zeitpunkt der Erstellung des ST.

Der AK kontrolliert die Erzeugung qualifizierter elektronischer Signaturen für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten. Bei festgestellten Abweichungen im Signaturprozess wird das Clientsystem über die Schnittstellen darüber informiert und alle Signaturen des Stapels verworfen. Der AK setzt den Sicherheitszustand des HBA, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers erlangt wurde, nach der Abarbeitung des Stapels zurück.

Anwendungshinweis 47: Ein Benutzer des Clientsystems ist dann für die Auslösung des Signaturprozesses einer Stapelsignatur autorisiert, wenn der Benutzer sich an dem eHealth-Kartenterminal gegenüber dem dieser Benutzeridentität zugeordneten Heilberufsausweis erfolgreich mit der PIN.QES authentisiert hat (vergl. [21]).

Anwendungshinweis 48: Ordnungsgemäße qualifizierte elektronische Signaturen sind solche fortgeschrittenen elektronischen Signaturen, die zu den Daten des Stapels mit dem Signaturschlüssel des Heilberufsausweises des autorisierten Benutzers des Clientsystems erzeugt wurden und zu dessen öffentlichen Signaturprüfschlüssel zum für die Signatur festgelegten Zeitpunkt ein gültiges qualifiziertes Zertifikat existiert. Dieser für die Signatur festgelegte Zeitpunkt bestimmt den Zeitpunkt der Prüfung der Gültigkeit des qualifizierten Zertifikats durch den AK. Es wird darauf hingewiesen, dass die Gültigkeit einer qualifizierte elektronische Signatur sich für den angegebenen Zeitpunkt der Signaturerstellung ergibt.

Anwendungshinweis 49: Der Konnektor setzt die Einfach- und die Stapelsignatur und die Komfortsignatur um. Die Sicherheitsziele des PP [16] wurden entsprechend um das Sicherheitsziel O.AK.Sig.Komfortsignatur ergänzt.

O.AK.Sig.Komfortsignatur Komfortsignatur

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen durch eine Komfortsignatur. Der AK steuert die einmalige Eingabe der QES-PIN bei Aktivierung des Komfortsignaturmodus für eine HBA-Kartensitzung am eHealth Kartenterminal und die Erzeugung der digitalen Signaturen durch den HBA. Die bei Aktivierung des Komfortsignatur-Modus übergebene User-ID der HBA-Kartensitzung wird dem Authentisierungskontext der HBA-Kartensitzung zugeordnet und dient der Authentisierung des Clientsystems bei der Erzeugung von Komfortsignaturen. Der AK authentisiert sich gegenüber dem HBA mit der Identität „SAK“. Die Kommunikation zwischen AK und HBA ist per Secure Messaging geschützt.

Der AK kontrolliert die Erzeugung qualifizierter elektronischer Signaturen für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten. Bei festgestellten Abweichungen im Signaturprozess wird das Clientsystem über die Schnittstellen darüber informiert und die erzeugte Signatur verworfen. Der AK setzt den Sicherheitszustand der HBA-Kartensitzung, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers bei der Aktivierung der Komfortsignatur erlangt wurde, nach Ablauf eines konfigurierten Zeitraumes, nach der Durchführung einer konfigurierten Anzahl von Komfortsignaturen oder bei Deaktivierung des Komfortsignatur-Modus zurück.

Anmerkung 5. Der secunet konnektor 2.0.0 unterstützt bis zu zwei parallele HBA-Kartensitzungen für die Komfortsignatur.

O.AK.Sig.Schlüsselinhaber Zuordnung des Signaturschlüssel-Inhabers

Bei der Überprüfung der signierten Daten stellt der AK fest, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist oder dass eine solche Zuordnung nicht möglich ist. Im Fall der qualifizierten elektronischen Signatur ist das Prüfergebnis dem Benutzer des Clientsystems über die Schnittstellen bereitzustellen.

O.AK.Sig.SignaturVerifizierung Verifizierung der Signatur

Der AK prüft zuverlässig die Korrektheit digitaler Signaturen und stellt das Ergebnis der Prüfung an der Schnittstelle zum Clientsystem zur Verfügung. Der AK unterstützt für die Signaturprüfung die kryptographische Algorithmen gemäß [13]. Der AK unterstützt Formate signierter Dokumente gemäß CadES, PAdES und XAdES. Schlägt die Prüfung der Signatur fehl, wurden die Daten mit einem kryptographisch schwachen Signaturalgorithmus erzeugt oder kann die Signaturprüfung nicht durchgeführt werden, so wird eine entsprechende Warnung ausgegeben.

O.AK.Sig.PrüfungZertifikat Prüfung des Signatur-Zertifikates

Bei der Überprüfung qualifiziert und nicht-qualifiziert signierter Daten prüft der AK die Gültigkeit dieser Zertifikate, auf denen die Signatur beruht, zum Zeitpunkt der Erstellung der Signatur und stellt das Ergebnis der Prüfung an der Schnittstelle zum Clientsystem zur Verfügung. Diese Prüfung schließt ein, ob die für qualifizierte Zertifikate verwendeten Signaturalgorithmen zum Signaturprüfungszeitpunkt gemäß [19] als kryptographisch sicher gelten bzw. galten.

4.2.3. Gesicherte Kommunikation / TLS Proxy

O.AK.LAN gesicherte Kommunikation im LAN der Leistungserbringer

Der EVG bietet eine gesicherte Kommunikationsverbindung zum Clientsystem an, so dass Angriffe auf die Kommunikation durch Abhören, Manipulieren und Vorgeben einer falschen Identität zwischen Clientsystemen und dem EVG in beiden Richtungen abgewehrt werden können, sofern die Funktionalität durch die Clientsysteme ebenfalls unterstützt wird. Der EVG bietet dazu folgende Sicherheitsfunktionalität:

Der Administrator kann durch Konfiguration sowohl

- eine nur Server-seitige Authentisierung des EVGs gegenüber den Clientsystemen aktivieren als auch
- eine gegenseitige Authentisierung zwischen Clientsystemen und EVG erzwingen.

- Schließlich kann die Authentisierung zwischen Clientsystemen und EVG auch vollständig ausgeschaltet werden. In diesem Fall muss der Administrator bzw. der Betreiber des Konnektors den Kommunikationskanal durch geeignete organisatorische Maßnahmen absichern.

Die gegenseitige Authentisierung zwischen Clientsystemen und EVG ist bei Auslieferung des EVGs voreingestellt.

Sofern eine Authentisierung zwischen Clientsystemen und EVG konfiguriert wurde, wird die Kommunikation mit den Clientsystemen hinsichtlich ihrer Vertraulichkeit und Integrität geschützt.

Der EVG authentisiert sich selbst gegenüber den Clientsystemen mit Hilfe von Schlüsselmaterial, welches auf dem Sicherheitsmodul gSMC-K gespeichert ist oder in den EVG importiert bzw. vom EVG generiert wurde.

Anwendungshinweis 50: Über die Administrations-Schnittstelle des EVG können Clientsysteme dem EVG bekannt gemacht und deren Schlüsselmaterial (Zertifikate) importiert werden. Das führt zu einer Whitelist von erlaubten Clients, aus der auch Einträge wieder entfernt werden können. Es kann auch Schlüsselmaterial (Zertifikate) für die TLS-Kommunikation vom EVG generiert, exportiert (für Server nur die Zertifikate) und importiert werden.

Anwendungshinweis 51: Der Endpunkt eines TLS-Kanals zwischen EVG und Clientsystemen kann sowohl in einem Terminal-Server liegen als auch in einem Client und damit näher am Arbeitsplatz des Nutzers.

O.AK.WAN gesicherte Kommunikation zwischen EVG und Fachdiensten

Der EVG bietet eine gesicherte Kommunikationsverbindung zu Fachdiensten bzw. Intermediären an, so dass Angriffe auf die Kommunikation durch Abhören, Manipulieren und Vorgeben einer falschen Identität zwischen Fachdiensten bzw. Intermediären und dem EVG in beiden Richtungen abgewehrt werden können, sofern die Funktionalität durch die Fachdienste bzw. Intermediäre ebenfalls unterstützt wird. Dazu können TLS Verbindungen zu Fachdiensten bzw. Intermediären auf- und abgebaut werden. Der EVG prüft die Authentizität des Server-Zertifikates (des Fachdienstes/Intermediärs). Eine Client-seitige Authentisierung des EVG kann mit einer SM-B erfolgen.

O.AK.VAUSGD Geschützte Kommunikation mit VAU-Instanz und SGD-HSM

Der EVG bietet eine gesicherte Kommunikationsverbindung mittels „VAU-Protokoll“ in die VAU-Instanz des ePA-Aktensystems und mittels „SGD-Protokoll“ in das SGD-HSM des Schlüsselgenerierungsdienst an, sodass das Abhören von Daten für diese Kommunikation unterbunden ist. Das VAU-Protokoll ist gemäß der Spezifikation [30] umgesetzt. Das SGD-Protokoll ist gemäß den Spezifikationen [48] und [30] umgesetzt.

4.2.4. Terminal- und Chipkartendienst

O.AK.exklusivZugriff	Alleinige Kontrolle von Terminal und Karte

Der AK stellt Methoden zur Verfügung, die es dem Benutzer ermöglichen, die alleinige Kontrolle über die verwendeten Kartenterminals und die verwendeten Chipkarten auszuüben. Nach Beendigung der Transaktion werden die Ressourcen wieder freigegeben.

O.AK.PinManagement	Management von Chipkarten-PINs

Der AK ermöglicht das Ändern, Aktivieren und Deaktivieren von PINs der Chipkarten, das Abfragen der Status von PINs der Chipkarten sowie das Entsperren gesperrter Chipkarten-PINs.

O.AK.IFD-Komm	Schutz der Kommunikation mit den eHealth-Kartenterminals

Der EVG authentisiert die eHealth-Kartenterminals, mit denen er gepaart ist, und schützt die Vertraulichkeit und Integrität seiner Kommunikation mit den eHealth-Kartenterminals durch einen entsprechend gesicherten Kanal. Der EVG stellt diesen Kanal bereit und kontrolliert dessen Nutzung.

Anwendungshinweis 52: Es ist vorgesehen, aber durch den EVG nur im Zusammenwirken mit den eHealth-Kartenterminals durchsetzbar (s. OE.AK.Kartenterminal), dass die gesamte Kommunikation der Geräte im LAN des Leistungserbringers mit den eHealth-Kartenterminals über den EVG erfolgt. Das Pairing des Konnektors und der eHKT als Teil der Terminalverwaltung zur gegenseitigen Authentisierung zum Aufbau und der Betrieb des TLS-Kanals sind in [27] beschrieben.

O.AK.Chipkartendienst	Chipkartendienste des AK

Der AK identifiziert Chipkarten an der ICCSN und zusätzlich im Fall der HBA, SMC und eGK den Chipkartentyp mit den in den Zertifikaten auf der Chipkarte enthaltenen Angaben.[23] Der AK stellt einen Sicherheitsdienst zur Authentisierung der eGK und zur gegenseitigen Authentisierung zwischen Chipkarten (Card-to-Card-Authentisierung) in den angeschlossenen eHealth-Kartenterminals bereit. Der AK gewährt den Zugriff auf Chipkarten in Abhängigkeit von deren Sicherheitszustand und der Sicherheitspolitik des Anwendungsfalls.

[23] Der Chipkartentyp (HBA, SMC und eGK) kann aus verschiedenen Quellen auf der jeweiligen Karte verlässlich bestimmt werden (bspw. CV-Zertifikat und X.509-Zertifikat). Bei der Personalisierung der Karten wird sichergestellt, dass die Konsistenz hinsichtlich des Kartentyps zwischen diesen Quellen gewahrt ist.

Anwendungshinweis 53: Eine erfolgreiche gegenseitige Card-to-Card-Authentisierung besagt nur, dass beide beteiligten Karten CVC aus derselben PKI besitzen und die Karten über die privaten Schlüssel zu den CVC verfügen. Folglich wird die Authentizität einer Chipkarte nur dann nachgewiesen oder widerlegt, wenn die andere Chipkarte bereits als authentisch bekannt ist. Der EVG stellt keinen eigenständigen, von der Nutzung einer bereits als authentisch bekannten Chipkarte unabhängigen Sicherheitsdienst zur Authentisierung von HBA und SMC-B bereit. Diese Authentizität der HBA und SMC-B in Kartenlesern des lokalen Netzes des Leistungserbringers ist durch den Leistungserbringer selbst zu gewährleisten, s. Sicherheitsziel für die Einsatzumgebung OE.AK.Karten.

O.AK.VAD	Schutz der Authentisierungsverifikationsdaten

Der AK steuert die lokale und entfernte Eingabe von Authentisierungsverifikationsdaten der Benutzer der Chipkarten. Der AK unterstützt den Benutzer der entfernten Eingabe bei der Identifizierung des zu benutzenden PIN-Terminals durch die sichere Bereitstellung einer hinreichend eindeutigen Jobnummer für das Clientsystem und der späteren Anzeige der vom Clientsystem übergebenen Jobnummer am PIN-Terminal, die dem identifizierten Arbeitsplatz zugeordnet ist. Der AK initiiert die Eingabe der Signatur-PIN und Signatur-PUK des Signaturschlüssel-Inhabers bzw. der Kartenhalter-PIN und Kartenhalter-PUK des Kartenhalters im sicheren PIN-Modus am PIN-Terminal und deren vertrauliche und integritätsgeschützte Übermittlung im Secure Messaging Kanal zwischen der SMC im PIN-Terminal zur VAD-empfangenden Chipkarte im Chipkarten-Terminal.

4.2.5. Verschlüsselungsdienste

O.AK.Enc	Verschlüsselung von Daten

Der AK verschlüsselt übergebene Daten gemäß der Verschlüsselungsrichtlinie der Fachanwendung bzw. des Anwendungsfalls für die über die Schnittstelle angegeben Empfänger, wenn deren Verschlüsselungszertifikate gültig sind. Es werden die Cryptographic Message Syntax [78] und XML-Encryption [79] unterstützt.

O.AK.Dec	Entschlüsselung von Daten

Der AK entschlüsselt Daten, wenn die Verschlüsselungsrichtlinie und der Sicherheitszustand der Chipkarten mit den benötigten Entschlüsselungsschlüsseln dies erlauben.

4.2.6. Fachmodule

O.AK.VSDM	Versichertenstammdatenmanagement

Für eine Verbindung zwischen dem VSDM Fachmodul (als Bestandteil des EVG) und dem Fachdienst VSDD bzw. Intermediär VSDM erzwingt der EVG auf Anforderung des VSDM Moduls den Aufbau und die Nutzung eines TLS Kanals mit gegenseitiger Authentisierung. Für eine Verbindung zwischen dem Fachdienst VSDD oder dem CMS und einer gesteckten Chipkarte im eHealth-KT im LAN der Leistungserbringer erzwingt das VSDM Fachmodul den Aufbau und die Nutzung eines Secure Messaging Kanals. Nach Abbau des Secure Messaging Kanals zwischen Chipkarte und Fachdienst wird der TLS- Kanal durch den EVG abgebaut.

Für alle Lesezugriffe auf geschützte Versichertenstammdaten (VSD) der eGK sowie für die Aktualisierung von VSD auf der eGK erzwingt das VSDM Fachmodul die Protokollierung auf der eGK.

O.AK.VZD	Kommunikation mit dem zentralen Verzeichnisdienst

Der Konnektor stellt einen gesicherten Kanal vom LDAP-Proxy zum zentralen Verzeichnisdienst der TI-Plattform (VZD) bereit und ermöglicht es, durch Nutzung des LDAP-Proxy, Daten aus dem VZD abzufragen.

4.3. Sicherheitsziele für die Umgebung des Netzkonnektors

Aus dem Schutzprofil BSI-CC-PP-0098 [16] sind folgende Sicherheitsziele für die Umgebung des Netzkonnektors übernommen. Dabei werden entsprechend dem Schutzprofil einige Sicherheitsziele für die Umgebung des Netzkonnektors bereits direkt vom Gesamtkonnektor oder dessen Umgebung erfüllt. Eine Abbildung der entsprechenden Sicherheitsziele aus 4.3 findet sich in Tabelle 10: Umgang mit Umgebungszielen des NK im EVG prüfen wieder.

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

OE.NK.RNG	Externer Zufallszahlengenerator

Die Umgebung stellt dem EVG einen externen Zufallszahlengenerator bereit, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klasse PTG.2 oder PTG.3 aus [11] liefert.

Anwendungshinweis 54: Der Zufallszahlengenerator der gSMC-K wird als physikalischer Zufallszahlengenerator der Klasse PTG.2 als (Re-)Seed-Generator für den Zufallszahlengenerator des Betriebssystems genutzt (GET RANDOM Kommando).

OE.NK.Echtzeituhr Echtzeituhr

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

Anwendungshinweis 55: Die Hardware des Konnektors muss eine Real Time Clock mit maximal zulässigem Drift von +/- 20ppm (part per million) zur Verfügung stellen (siehe Kapitel 1.3.6). Dies entspricht einer maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über 20 Tage.

Die Freilaufgenauigkeit garantiert eine Abweichung von weniger als 2 Sekunden pro Tag, so dass bei einer Synchronisation spätestens alle 24 Stunden der Zeitdienst des Konnektors um maximal 2 Sekunden ungenau ist.

Anwendungshinweis 56: Das Umgebungsziel des Netzkonnektors OE.NK.Echtzeituhr wurde aus dem Schutzprofil BSI-CC-PP-0098 [16] entnommen und ist dem Netzkonnektor zugeordnet. Es ist nur zur Vollständigkeit hier aufgeführt, siehe dazu auch *Anwendungshinweis 54* im Schutzprofil. OE.NK.Echtzeituhr wird durch das Umgebungsziel OE.AK.Echtzeituhr des Anwendungskonnektors eingeschlossen. Siehe auch Tabelle 10.

OE.NK.Zeitsynchro Zeitsynchronisation

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

OE.NK.gSMC-K Sicherheitsmodul gSMC-K

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

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

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

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

Anwendungshinweis 57: Der Konnektor verwendet nur von der gematik zugelassene Sicherheitsmodule gSMC-K, siehe 1.3.6.

OE.NK.KeyStorage Sicherer Schlüsselspeicher

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

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

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

Anwendungshinweis 58: Der EVG verwendet als sicheren Schlüsselspeicher die gSMC-K. Darin sind auch die privaten Schlüssel zur Entschlüsselung des geräteindividuellen CFS-Schlüssels abgelegt. Die Sicherheit der im CFS abgelegten Daten ist damit wieder auf den sicheren Schlüsselspeicher der gSMC-K zurückzuführen.

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

Anwendungshinweis 59: Das Umgebungsziel des Netzkonnektors OE.NK.KeyStorage wird ganz oder teilweise durch die gSMC-K erbracht. Siehe auch Tabelle 10.

OE.NK.AK	Korrekte Nutzung des EVG durch Anwendungskonnektor

Anwendungskonnektoren müssen zu schützende Daten der TI und der Bestandsnetze, die durch Dienste gemäß § 291a SGB V [14] verarbeitet werden sollen, in korrekter Weise an den EVG übergeben, damit der EVG zu schützende Daten der TI und der Bestandsnetze über den entsprechenden VPN-Tunnel für Dienste gemäß § 291a SGB V versenden kann.

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

Anwendungshinweis 60: Siehe auch A.NK.AK.

Anwendungshinweis 61: Das Umgebungsziel des Netzkonnektors OE.NK.AK wurde aus dem Schutzprofil BSI-CC-PP-0098 [16] entnommen und ist dem Netzkonnektor zugeordnet. Es ist nur zur Vollständigkeit hier aufgeführt, siehe dazu auch *Anwendungshinweis 54* im Schutzprofil. Siehe auch Tabelle 10.

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

Die Hersteller von Clientsystemen müssen ihre Produkte so gestalten, dass diese den Konnektor für Dienste gemäß § 291a SGB V [14] korrekt aufrufen. Aufrufe von Diensten gemäß § 291a SGB V [14] müssen über den Anwendungskonnektor erfolgen. Der Zugriff auf Bestandsnetze und offene Fachanwendungen erfolgt nur durch aktive Komponenten im LAN in den vorgesehenen IP-Adressbereichen.

OE.NK.Admin_EVG	Sichere Administration des Netzkonnektors

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

Anwendungshinweis 62: Der EVG verfügt zur Identifikation über eine eindeutige Seriennummer. Es wird organisatorisch sichergestellt, dass die Seriennummer bei Verlust des Gerätes noch vorliegt oder rekonstruiert werden kann, damit das Gerät bei der Verlustmeldung eindeutig identifiziert werden kann, so dass weitergehende Schritte (z. B. Sperrung des zugehörigen Zertifikats) eingeleitet werden können.

OE.NK.Admin_Auth *Authentisierung des Administrators*

OE.NK.Admin_Auth aus PP [17] ist für den EVG nicht relevant, da der EVG die Authentisierung des Administrators selbst durchführt, siehe O.NK.Admin_Auth und Anwendungshinweis 63:

Anwendungshinweis 63: Der Konnektor setzt eine übergreifende Administratorrolle um. Die Authentisierung des Konnektor-Administrators wird dabei vom Netzkonnektor vorgenommen. Das Umgebungsziel OE.NK.Admin_Auth des PP [17] wurde in das EVG-Ziel **O.NK.Admin_Auth** umgewandelt. Die funktionale Anforderung FMT_MSA.4/NK PP [17] wurde nicht in diesem ST übernommen, dafür wurde mit FIA_UAU.1/NK.SMR eine die Authentisierung des Administrators modellierende Anforderung in das ST aufgenommen.

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

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

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

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

OE.NK.phys_Schutz Physischer Schutz des EVG[24]

Die Sicherheitsmaßnahmen in der Umgebung müssen den Konnektor (während aktiver Datenverarbeitung im Konnektor) vor physischen Zugriff Unbefugter schützen. Befugt sind dabei nur durch den Betreiber des Konnektors namentlich autorisierte Personen (z. B. Leistungserbringer, ggf. medizinisches Personal). Sowohl während als auch außerhalb

[24] Der EVG ist ein Einbox-Konnektor und kein verteilt betriebener Mehrkomponenten-Konnektors.

aktiver Datenverarbeitung im Konnektor müssen die Sicherheitsmaßnahmen in der Umgebung sicherstellen, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass die einzuleitenden materiellen, organisatorischen und/oder personellen Maßnahmen größeren Schaden abwehren.

Anwendungshinweis 64: Siehe auch A.NK.phys_Schutz resp. **O.NK.Schutz**.

Anwendungshinweis 65: Das Umgebungsziel OE.NK.phys_Schutz des Netzkonnektors und das Umgebungsziel OE.AK.phys_Schutz des Anwendungskonnektors sind identisch formuliert. Letzteres fordert physischen Schutz des gesamten Konnektors. Siehe auch Tabelle 10.

OE.NK.sichere_TI Sichere Telematikinfrastruktur-Plattform

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

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

Alle Administratoren in der Telematikinfrastruktur müssen fachkundig und vertrauenswürdig sein.

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

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

Anwendungshinweis 66: Siehe auch A.NK.kein_DoS.

OE.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

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

Er administriert die Anwendungskonnektoren in sicherer Art und Weise.

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

Anwendungshinweis 67: Das Umgebungsziel des Netzkonnektors OE.NK.Betrieb_AK wurde aus dem Schutzprofil BSI-CC-PP-0098 [16] entnommen und ist dem Netzkonnektors zugeordnet. Es ist nur zur Vollständigkeit hier aufgeführt, siehe dazu auch *Anwendungshinweis 65* im Schutzprofil. Dieses Sicherheitsziel für die Umgebung des NK wird abgebildet auf die Sicherheitsziele OE.AK.Plattform und OE.AK.Personal des AK. Siehe auch Tabelle 10.

OE.NK.Betrieb_CS Sicherer Betrieb der Clientsystems

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

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

Er administriert die Clientsysteme in sicherer Art und Weise.

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

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

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

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

OE.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

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

OE.NK.SIS	Sicherer Internet Service

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

Die Administration des Sicheren Internet Service muss dafür sorgen, dass dieses System frei von Schadsoftware gehalten wird, so dass keine Angriffe über den sicheren VPN-Kanal zum Konnektor von diesem Zugangspunkt ausgehen. Im Fall der Nutzung des SIS als VPN-Konzentrator impliziert dies, dass die VPN-Schlüssel auf Seiten des Sicheren Internet Service geheim gehalten werden müssen und nur für die rechtmäßigen Administratoren zugänglich sein dürfen.

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

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

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

Hinweis: Das Sicherheitsziel für die Umgebung des Netzkonnektors OE.NK.SW-Update ist identisch zum Sicherheitsziel für die Umgebung des Anwendungskonnektors OE.AK.SW-Update. Siehe auch Tabelle 10.

Einige der vorgenannten Sicherheitsziele für die Umgebung des Netzkonnektors aus [16], Kapitel 4.3 werden durch den Gesamtkonnektor bereits auf anderer Weise umgesetzt. Diese Sicherheitsziele wurden aus dem NK-PP [17] in das zugrundliegende Schutzprofil nur zur Vollständigkeit übernommen. In den Sicherheitsvorgaben (Security Target) werden sämtliche Umgebungsziele des Schutzprofils [16] vollständig übernommen. Tabelle 10 enthält diese Sicherheitsziele zusammen mit der Erklärung, wie sie entsprechend dem zugrundeliegenden Schutzprofil behandelt werden.

Sicherheitsziel aus BSI-CC-PP-0097 [17]	**Bemerkungen**
OE.NK.KeyStorage	*Sicherer Schlüsselspeicher:* Dieser Schutz wird durch die gSMC-K erbracht, also entsprechend nicht vom EVG sondern von der Umgebung
OE.NK.AK	*Korrekte Nutzung des Netzkonnektors durch Anwendungskonnektor* Das Umgebungsziel des Netzkonnektors wurde aus dem Schutzprofil BSI-CC-PP-0097 [17] des Netzkonnektors in das zugrundeliegende Schutzprofil [16] übernommen und ist nur zur Vollständigkeit in den Sicherheitsvorgaben enthalten. Die korrekte Nutzung der NK-Schnittstellen durch den AK ist

Sicherheitsziel aus BSI-CC-PP-0097 [17]	Bemerkungen
	Gegenstand der Evaluierung des EVG (u.a. CC-Klassen ADV und ATE).
OE.NK.Admin_Auth	*Authentisierung des Administrators:* Dieses Sicherheitsziel wird abgebildet auf das Sicherheitsziel O.AK.Admin des Anwendungskonnektors. Dies ist konsistent zum Schutzprofil BSI-CC-PP-0097, weil der Anwendungskonnektor des vorliegenden Schutzprofiles zur Umgebung des EVG aus BSI-CC-PP-0097 gehört.
OE.NK.Betrieb_AK	*Sicherer Betrieb des Anwendungskonnektors*: Dieses Sicherheitsziel für die Umgebung des NK wird abgebildet auf die Sicherheitsziele OE.AK.Plattform und OE.AK.Personal für die Umgebung des EVG, sowie die Sicherheitsziele O.AK.Admin und O.AK.EVG_Modifikation des AK. Die korrekte Nutzung der NK-Schnittstellen durch den EVG ist Gegenstand der Evaluierung des EVG.
OE.NK.phys_Schutz	*Physischer Schutz des EVG*. A.NK.phys_Schutz und A.phys_Schutz sind identisch formuliert. OE.NK.phys_Schutz und OE.phys_Schutz sind ebenfalls identisch formuliert. A.NK.phys_Schutz OE.NK.phys_Schutz beziehen sich aber nur auf den Netzkonnektor als Teil des aktuellen EVG, während sich A.phys_Schutz und OE.phys_Schutz auf den gesamten EVG beziehen.
OE.NK.Echtzeituhr	Für den Konnektor wurde OE.AK.Echtzeituhr aufgenommen.

Tabelle 10: Umgang mit Umgebungszielen des NK im EVG

4.4. Sicherheitsziele für die Umgebung des Anwendungskonnektors

Über die in Abschnitt 4.3 aufgeführten Sicherheitsziele für die Umgebung des Netzkonnektors hinaus werden folgende Sicherheitsziele für die Umgebung des EVG definiert:

OE.AK.Versicherter Sorgfaltspflichten des Versicherten

Der Versicherte darf seine eGK nur dann und nur dort einem HBA-Inhaber oder einem seiner Mitarbeiter aushändigen, wenn er diesem Zugriff auf seine Daten gewähren will. Nach Abschluss der Konsultation nimmt er seine eGK wieder an sich.

OE.AK.HBA-Inhaber Vertrauenswürdigkeit und Sorgfaltspflichten des HBA-Inhabers

Der HBA-Inhaber und seine Mitarbeiter sind in Bezug auf den Umgang mit den ihm bzw. ihnen anvertrauten zu schützenden Daten vertrauenswürdig. Alle Leistungserbringer, die Zugriff auf medizinische Daten haben, welche auf Clientsystemen lokal gespeichert werden, gehen verantwortungsvoll mit diesen Daten um.

Der Betreiber des Konnektors administriert seine IT-Umgebung in einer Art und Weise, die Missbrauchsmöglichkeiten minimiert. Der HBA-Inhaber verwendet seinen HBA nur in IT-Umgebungen, die wie im vorigen Satz beschrieben sicher administriert werden.

OE.AK.SMC-B-PIN Freischaltung der SMC-B

Der Karteninhaber stellt sicher, dass die SMC-B nur freigeschaltet ist, wenn sie und der Konnektor unter seiner Kontrolle arbeiten. Wenn der Karteninhaber keine Kontrolle mehr über den Konnektor oder die SMC-B hat, setzt er die Freischaltung der SMC-B zurück (z.B. durch Ausschalten des Kartenterminals oder Ziehen der Chipkarte).

OE.AK.sichere_TI Sichere Telematikinfrastruktur-Plattform

Die zentrale Telematikinfrastruktur-Plattform muss als vertrauenswürdig angesehen werden, d.h., es gibt keine Angriffe aus der zentralen Telematikinfrastruktur-Plattform und es ist sichergestellt, dass die zentrale Telematikinfrastruktur-Plattform die ihr anvertrauten Daten / Informationen nicht missbraucht. Zudem ist gewährleistet, dass die Dienste zentrale TI-Plattform die kryptographischen Vorgaben aus [16] erfüllen. Die Administration der Telematikinfrastruktur sorgt dafür, dass die Server in der Telematikinfrastruktur frei von Schadsoftware gehalten werden, so dass über bestehende Kanäle zum AK keine Angriffe auf den AK erfolgen. Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

OE.AK.Fachdienste vertrauenswürdige Fachdienste und zentrale Dienste der TI-Plattform

Fachdienste, zentrale Dienste der TI-Plattform und deren Intermediäre werden als vertrauenswürdig angesehen. Es erfolgen keine Angriffe über bestehende Kommunikationskanäle auf den AK. Die Verbindungsschlüssel auf Seiten der Fachdienste, zentralen Dienste und Intermediäre werden geheim gehalten und sind nur für die rechtmäßigen Administratoren zugänglich. Fachdienste, zentrale Dienste, Intermediäre und deren Schlüsselmaterial werden vor Angriffen geschützt. Es wird angenommen, dass nur berechtigte Entitäten über die Telematikinfrastruktur auf Fachdienste, zentrale Dienste und Intermediäre zugreifen können. Dies wird durch technische oder organisatorische

Maßnahmen abgesichert. Wird dennoch ein Fachdienst/zentraler Dienst/Intermediär und/oder sein Schlüsselmaterial erfolgreich angegriffen, so werden die betroffenen Schlüssel zeitnah gesperrt. Alle genutzten kryptographischen Sicherheitsmechanismen werden im Einklang mit den relevanten Vorgaben des Dokuments TR-03116-1 [19] implementiert.

Anwendungshinweis 68: Im Fall der Fachanwendung VSDD müssen insbesondere die Komponenten VSDD-Dienst und CMS in der beschriebenen Weise vertrauenswürdig sein. Kommunikationskanäle zwischen VSDD bzw. CMS und gesteckten eGK in einem eHealth KT in dem lokalen Netz der Leistungserbringer müssen durch Secure Messaging bezüglich Vertraulichkeit und Authentizität geschützt werden. Das dazu verwendete Schlüsselmaterial muss in der oben beschriebenen Weise geschützt werden.

OE.AK.Admin_EVG Sichere Administration des Anwendungskonnektors

Der Betreiber des Konnektors sorgt dafür, dass administrative Tätigkeiten in Übereinstimmung mit der Administrator-Dokumentation des EVG durchgeführt werden. Insbesondere wird für diese Tätigkeiten vertrauenswürdiges und hinreichend geschultes Personal eingesetzt. Der Administrator handelt nur im Sinne des verantwortlichen Leistungserbringers bzw. Konnektor-Betreibers und in dessen Auftrag. Der Administrator ist verantwortlich dafür, die automatische Aktualisierung des Konnektor zu konfigurieren und hat im Falle des manuellen anwendens von Aktualisierungen das Recht das Update anzustoßen. Der Administrator hält Authentisierungsinformationen und –token geheim bzw. gibt diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token). Der Administrator implementiert nur Vertrauenswürdige Komponenten (insbesondere eHealth-Kartenterminals) im Informationsmodell. Der Leistungserbringer als Nutzer des Konnektors hat die Verantwortung, die Eignung der aktuell genutztenen Konnektorfirmware-Version zu prüfen.

Anwendungshinweis 69: Die Information der Benutzer des AKs, welche Firmware-Version aktuell genutzt wird, kann vom Administrator über die Managementschnittstelle ausgelesen werden. Der Konnektor unterstützt die automatische Aktualisierung („AutoUpdate“). Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartenterminals organisatorisch genschützt werden.

OE.AK.Admin_Konsole sichere Administratorkonsole

Der Betreiber des EVG stellt sicher, dass die Administrationskonsole (die Benutzerschnittstelle zur Administration des EVG) vertrauenswürdig ist. An dieser Konsole vom Administrator eingegebene Authentisierungsgeheimnisse (z. B. Passwort, PIN, Passphrase) werden von der Konsole vertraulich behandelt und nicht zwischengespeichert. Die Konsole stellt Bildschirminhalte unverfälscht dar.

OE.AK.Kartenterminal sicheres Kartenterminal

Als Kartenterminal werden nur Geräte eingesetzt, die nach dem Schutzprofil für das eHealth-Kartenterminals der elektronischen Gesundheitskarte [22] evaluiert und zertifiziert sind. Dies beinhaltet insbesondere, dass das Kartenterminal

(1) die gegenseitige Authentisierung mit dem EVG und Nutzung eines TLS-Kanals für die festgelegten SICCT-Kommandos erzwingt und seine Authentisierung mit Pairing-Geheimnis unterstützt,

(2) die Kommunikation nur mit höchstens einer Gegenstelle (über höchstens einem TLS-Kanal) zum Empfang von SICCT-Kommandos und zum Senden der dazugehörigen Antworten erlaubt,

(3) dem Nutzer vom Kartenleser angezeigt wird, wenn dieser sich im sicheren PIN-Eingabemodus befindet,

(4) Kommandos zur Erzeugung geschützter Kommandos zur PIN-Prüfung, zum PIN-Wechsel und zum Rücksetzen des Fehlbedienungszählers im sicheren PIN-Modus unterstützt,

(5) die Tastatureingabedaten nur temporär im Kartenleser während der Eingabe gespeichert und nach der Übergabe an die Chipkarte wieder gelöscht werden,

(6) die gesteckten Chipkarten bei Abbau des TLS-Kanals zurücksetzt (Reset), und

(7) die Vorgaben der TR-03116-1 [16] erfüllt.

OE.AK.Plattform sichere Plattform

Die Plattform des EVG stellt dem EVG eine Ausführungsumgebung zur Verfügung, die den Konnektor selbst (z. B. seinen ausführbaren Code), die von ihm verarbeiteten Daten (sowohl flüchtige als auch ggf. persistent gespeicherte Daten) und die Fachmodule vor dem Zugriff durch Dritte (andere Programme, Prozesse, IT-Systeme o. ä.) schützt.

OE.AK.SecAuthData Schutz der Authentisierungsdaten

Die Benutzer schützen ihre Authentisierungsverifikationsdaten, d. h. die PIN und PUK der Chipkarten sowie Passwörter für die Authentisierung gegenüber dem EVG, vor Offenbarung und Missbrauch. Der Chipkarteninhaber darf seine PIN nur dann an einem Kartenterminal eingeben, wenn der initiierte Anwendungsfall dies erfordert und das Kartenterminal dem Chipkarteninhaber einen sicheren PIN-Eingabemodus anzeigt. Wird der Chipkarteninhaber von einem Kartenterminal zur PIN-Eingabe aufgefordert, ohne dass das Kartenterminal gleichzeitig den sicheren PIN-Eingabemodus anzeigt, muss der Chipkarteninhaber den Vorgang abbrechen und darf seine PIN nicht eingeben. Der Chipkarteninhaber kontrolliert, dass die PIN-Eingabe-Aufforderung (einschließlich Jobnummer) konsistent sowohl in seiner Clientsoftware, als auch auf dem PIN-Kartenterminal angezeigt wird.

OE.AK.phys_Schutz Physischer Schutz des EVG

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

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

OE.AK.Personal Qualifiziertes und vertrauenswürdiges Personal

Durch den Einsatz von qualifiziertem und vertrauenswürdigem Personal werden Fehler und Manipulationen bei Installation, Betrieb, Nutzung, Wartung und Reparatur des EVG ausgeschlossen. Das Personal kontrolliert, ob der EVG sicherheitstechnische Veränderungen anzeigt, insbesondere nutzen die Benutzer des EVG die Möglichkeit, die Integrität des EVG durch ein besonders zu schützendes Testprogramm zu überprüfen.

OE.AK.SMC Nutzung geeigneter SMC-B und gSMC-KT

Es werden nur solche Chipkarten mit privaten Schlüsseln und CVC als SMC-B bzw. gSMC-KT und den relevanten Rollen für die dazugehörigen öffentlichen Schlüssel ausgestattet, wenn das Betriebssystem nach dem dafür vom BSI veröffentlichten Schutzprofilen evaluiert und zertifiziert sowie deren Objektsystem getestet wurden. Für die SMC Typ B wird gemäß Schutzprofil [15] insbesondere gewährleistet, dass die SMC-B für die Benutzung des Signaturschlüssels, des Entschlüsselungsschlüssels und der privaten Authentisierungsschlüssel als SMC-B die erfolgreiche Authentisierung des Karteninhabers fordert. Die gSMC-KT kontrollieren den Zugriff auf das Schlüsselmaterial für den Trusted Channel zwischen einem eHealth-Kartenterminal und dem EVG. Die SMC verwenden nur sichere kryptographische Algorithmen gemäß [19].

Die genutzte SMC hat eine TR-Zertifizierung nach BSI TR-03144 erfolgreich durchlaufen (Nachweis der vertrauenswürdigen Initialisierung) und die Personalisierung der SMC ist sicher.

Der Chipkartentyp SMC kann aus verschiedenen Quellen auf der jeweiligen Karte verlässlich bestimmt werden (bspw. CV-Zertifikat und X.509-Zertifikat). Bei der Personalisierung der Karten muss sichergestellt sein, dass die Konsistenz hinsichtlich des Kartentyps zwischen diesen Quellen gewahrt ist.

OE.AK.gSMC-K Nutzung einer gSMC-K

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

Die gSMC-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptographische Identität des EVG repräsentiert und von ihm verwendet wird. Es führt kryptographische Operationen mit diesem Schlüsselmaterial durch, ohne dass das Schlüsselmaterial den sicheren Schlüsselspeicher dazu verlassen muss.

Die gSMC-K ist durch die gematk zugelassen.

Die genutzte gSMC-K hat eine TR-Zertifizierung nach BSI TR-03144 erfolgreich durchlaufen (Nachweis der vertrauenswürdigen Initialisierung) und die Personalisierung der gSMC-K ist sicher.

OE.AK.eGK Nutzung geeigneter eGK

Chipkarten werden nur dann mit privaten Schlüsseln und CVC als „elektronische Gesundheitskarten“ (eGK) und der relevanten Rolle für den dazugehörigen öffentlichen Schlüssel ausgestattet, wenn deren Betriebssystem nach dem dafür vom BSI veröffentlichten Schutzprofil [15] evaluiert und zertifiziert sowie deren Objektsystem getestet wurden. Dies beinhaltet insbesondere, dass die eGK

(1) für die Benutzung des Entschlüsselungsschlüssels PrK.CH.ENC die erfolgreiche Authentisierung des Karteninhabers erfordert,

(2) für die Benutzung des Entschlüsselungsschlüssels PrK.CH.ENCV die erfolgreiche Authentisierung des Karteninhabers oder einer Card-to-Card-Authentisierung mit festgelegten Rollen erfordert,

(3) nur sichere kryptographische Algorithmen gemäß [19] verwendet.

Der Chipkartentyp eGK kann aus verschiedenen Quellen auf der jeweiligen Karte verlässlich bestimmt werden (bspw. CV-Zertifikat und X.509-Zertifikat). Bei der Personalisierung der Karten muss sichergestellt sein, dass die Konsistenz hinsichtlich des Kartentyps zwischen diesen Quellen gewahrt ist.

OE.AK.HBA Nutzung einer qualifizierten Signaturerstellungseinheit

Chipkarten werden nur dann mit privaten Schlüsseln und CVC als Heilberufsausweis und den relevanten Rollen für die dazugehörigen öffentlichen Schlüssel ausgestattet, wenn deren Betriebssystem nach dem dafür vom BSI veröffentlichten Schutzprofil [15] und der Spezifikation des Objektsystems [35] evaluiert sowie als qualifizierte Signaturerstellungseinheit für qualifizierte elektronische Signaturen nach eIDAS zertifiziert

wurde. Für die Erzeugung einer qualifizierten elektronischen Signatur verfügt der HBA über einen Signaturschlüssel und einen Signaturprüfschlüssel mit einem zum Zeitpunkt der Signatur gültigen qualifizierten Zertifikat. Dies beinhaltet auch, dass der HBA

(1) für die Benutzung des Signaturschlüssels die erfolgreiche Authentisierung des Signaturschlüssel-Inhabers erfordert;

(2) die DTBS für die Stapelsignatur nur in einem Secure Messaging Kanal akzeptiert werden, der durch eine mit C.SAK.AUTD_CVC authentisierte Gegenstelle aufgebaut wurde;

(3) für die Benutzung des Entschlüsselungsschlüssels die erfolgreiche Authentisierung des Karteninhabers erfordert und

(4) nur sichere kryptographische Algorithmen gemäß [19] verwendet.

Der Chipkartentyp HBA kann aus verschiedenen Quellen auf der jeweiligen Karte verlässlich bestimmt werden (bspw. CV-Zertifikat und X.509-Zertifikat). Bei der Personalisierung der Karten muss sichergestellt sein, dass die Konsistenz hinsichtlich des Kartentyps zwischen diesen Quellen gewahrt ist.

OE.AK.Karten Chipkarten im LAN des Leistungserbringers

Der Leistungserbringer gewährleistet, dass nur authentische HBA und SMC-B in den Kartenlesern seines lokalen Netzes verwendet werden. Daten der eGK, die vor der Authentisierung der eGK gegenüber dem Konnektor gelesen werden, dürfen nur zur Identifizierung einer gesteckten Karte anhand des Kartenhandles verwendet werden. Elektronisch gespeicherte personenbezogene Daten auf der eGK dürfen nur nach erfolgreicher Authentisierung der eGK gegenüber dem Konnektor verwendet werden.

OE.AK.PKI PKI für Signaturdienste, Verschlüsselung und technische Komponenten

Der AK erhält Zugriff auf alle notwendigen Informationen, um zu entscheiden, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Dies beinhaltet auch die Verfügbarkeit einer stets aktuellen BNetzA-VL. Der Trusted Service Provider (TSP) sichert die Verfügbarkeit von OCSP-Diensten für die Zertifikate und einer stets aktuellen BNetzA-VL für die Zertifikate der qualifizierten elektronischen Signatur mit dem HBA, für Zertifikate für andere Signaturen und für Verschlüsselungszertifikate. Es werden CV Zertifikate nur für solche technischen Komponenten ausgestellt, die den technischen Spezifikationen entsprechen und – wenn vorgeschrieben – zertifiziert wurden. Für alle PKI werden die öffentlichen Schlüssel, bzw. Zertifikate der Vertrauensanker auf vertrauenswürdigem Weg verteilt.

Der Betreiber des TSL-Dienstes sichert zu, dass nur die richtigen BNetzA-VL Signer-Zertifikate in die TSL eingebracht werden.

OE.AK.Clientsystem sichere Clientsysteme

Die Clientsysteme, die mit dem EVG kommunizieren, müssen als vertrauenswürdig angesehen werden, d.h., es gibt keine Angriffe aus den Clientsystemen und es ist sichergestellt, dass sie die ihr anvertrauten Daten / Informationen nicht missbrauchen. Sofern ein Clientsystem eine gesicherte Kommunikation mit dem EVG unterstützt, muss das Schlüsselmaterial zum Aufbau und Betrieb des sicheren Kommunikationskanals adäquat geschützt werden. Dies gilt auch bei Verwendung von Terminal-Servern: Hier werden die Terminal-Server und die genutzten Thin-Clients in der angegebenen Weise als vertrauenswürdig angesehen.

Alle genutzten kryptographischen Sicherheitsmechanismen werden im Einklang mit den relevanten Vorgaben des Dokuments TR-03116-1 [19] implementiert.

Bei Verwendung der Komfortsignatur dient die User-ID zur Authentisierung des Clientsytems gegenüber dem Konnektor. Die User-ID muss vom Clientsystem sicher generiert werden. Die Authentifizierung des HBA-Inhabers für die Komfortsignatur muss vom Clientsystem vorgenommen werden.

OE.AK.ClientsystemKorrekt Clientsysteme arbeiten korrekt und unterstützen das Informationsmodell

Das Clientsystem arbeitet korrekt. Es führt fachliche Anwendungsfälle korrekt durch und nutzt die korrekten Daten. Es übergibt dem EVG die korrekten (vom Leistungserbringer intendierten) Daten. Sofern ein fachlicher Anwendungsfall durchgeführt werden soll, der einen HBA erfordert, identifiziert das Clientsystem den HBA-Inhaber bzw. den zu verwendenden HBA und das zuständige Fachmodul. Der Betreiber des Konnektors muss sicherstellen, dass die in seiner Umgebung betriebene Clientsystem-Software die Leistungserbringer (HBA-Inhaber) korrekt authentisiert.

Das Clientsystem dient dem Leistungserbringer als Benutzerschnittstelle zum Konnektor. Es übermittelt die vom Leistungserbringer gewünschten Aufrufe an den Konnektor.

Beim Aufruf des Konnektors mit einem Kartenzugriff übergibt das Clientsystem einen geeigneten Satz von Parametern, anhand dessen der Konnektor die Zuweisung oder Verweigerung von Sicherheitsstatus vornehmen kann.

Das Clientsystem kontrolliert den Zugriff auf die Entschlüsselungsfunktion des Konnektors, so dass keine unkontrollierten Entschlüsselungen (ohne Zustimmung des HBA-Inhabers, z. B. durch nicht autorisiertes medizinisches Personal) möglich sind. Das Clientsystem kontrolliert den Zugriff auf die Verschlüsselungsfunktion des Konnektors, sodass keine nicht intendierten Verschlüsselungen oder nicht intendierte Empfänger an den Konnektor übergeben werden.

Das Clientsystem stellt Rückmeldungen, Warnungen und Fehlermeldungen des Konnektors sowie über den Systeminformationsdienst gemeldete kritische Betriebszustände korrekt, sofort und verständlich dar.

Das Clientsystem stellt im Rahmen der Erzeugung und Prüfung einer QES die Dokumente, Zertifikate, Jobnummer und Fortschrittsanzeige der Stapelsignatur korrekt und

vertrauenswürdig dar und ermöglicht die Nutzung der vom AK angebotenen Abbruchfunktion der Stapelsignatur.

OE.AK.Benutzer_Signatur Prüfung zu signierender und zu prüfender Dokumente vor der Übermittlung an den AK

Der Benutzer des Clientsystems muss vor der Übermittlung an den AK sicherstellen, dass er nur solche Daten zur Signaturerzeugung und zur Signaturprüfung über sein Clientsystem an den AK übergibt, welche er auch tatsächlich signieren bzw. verifizieren will.

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

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

Anwendungshinweis 70: Update-Dateien anderer Komponenten wie der Kartenterminals werden hier nicht erfasst

OE.AK.Echtzeituhr Bereitstellung einer Echtzeituhr

Die IT-Umgebung stellt dem EVG eine Echtzeituhr zur Verfügung, die für die EVG-Sicherheitsdienste zur Signaturerstellung und Protokollierung verwendet werden kann.

Anwendungshinweis 71: Entsprechend Konnektor-Spezifikation [27] ist gefordert, dass falls LU_Online nicht aktiviert ist (MGM_LU_Online=Disabled), sichergestellt werden muss, dass der maximale zulässige Fehler von +/- 20ppm (part per million) gegenüber einer Referenzuhr nicht überschritten wird. Dies entspricht einer maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über 20 Tage.

4.5. Erklärung der Sicherheitsziele

4.5.1. Überblick über die Sicherheitsziele des Netzkonnektors

Die folgende Tabelle 11 bildet die Bedrohungen (Threats), organisatorischen Sicherheitspolitiken (OSPs) und Annahmen (Assumptions) auf Sicherheitsziele für den Netzkonnektor und dessen Umgebung ab.

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

Tabelle 11: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen

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

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

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

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

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

Anwendungshinweis 72: Die Inhalte in Tabelle 11 und im folgenden Erklärungstext (4.5.3) wurden aus dem PP [16] übernommen. Hierbei wurden die optionalen Zuordnungen, im PP markiert durch (x), entsprechend übernommen oder entfernt.

4.5.2. Überblick über die Sicherheitsziele des Anwendungskonnektors

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.VAUSGD	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD	O.NK.Zeitdienst
T.AK.DTBS			X						X																					
T.AK.VAD			X			X																								
T.AK.LAN.eHKT		X	X																											
T.AK.LAN.CS																			X											
T.AK.WAN.TI																				X										
T.AK.LAN.Admin		X																												
T.AK.Kanal_Missbrauch		X	X						X										X	X					X					
T.AK.Mani.EVG					X													X				X	X	X						X
T.AK.Mani.Client																						X	X				X			X
T.AK.Mani.TI																						X	X							X
T.AK.Mani.ExternerDienst																						X	X							X
T.AK.Mani.Chipkarte																						X	X	X			X			X
T.AK.Mani.Terminal																						X	X	X			X			X
T.AK.Mani.AdminKonsole		X																				X	X							X

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.VAUSGD	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD	O.NK.Zeitdienst
T.AK.MissbrauchKarte																						X	X	X		X	X			X
T.AK.Fehlbedienung																														
OSP.AK.MedSoc_Data			X				X	X		X	X		X	X	X	X	X		X	X					X		X			
OSP.AK.Konn_Spez		X	X			X	X	X		X		X	X	X								X	X	X	X	X	X			X
OSP.AK.KryptAlgo	X																													
OSP.AK.SW-Update		X																				X	X	X						X
OSP.AK.EVG_Modification					X																	X	X							X
OSP.AK.SC_Sign										X	X	X	X	X																
OSP.AK.SC_Authorized						X			X																					
OSP.AK.SC_SVAD						X																								
OSP.AK.SC_UnalteredData									X			X	X	X																
OSP.AK.SV_Certificate															X															
OSP.AK.SV_Signatory																X														
OSP.AK.SV_Unaltered_Data																	X													
OSP.AK.Encryption							X	X																						
OSP.AK.CardService				X		X																								
OSP.AK.Fachanwendungen																												X	X	
OSP.AK.VAUSGD																					X									

Tabelle 12: Abbildung der Sicherheitsziele des EVG auf Bedrohungen und OSPs

	OE.AK.Kartenterminal	OE.AK.Plattform	OE.AK.phys_Schutz	OE.AK.SecAuthData	OE.AK.Personal	OE.AK.HBA	OE.AK.SMC	OE.AK.eGK	OE.AK.Karten	OE.AK.PKI	OE.AK.Echtzeituhr	OE.AK.Versicherter	OE.AK.HBA-Inhaber	OE.AK.SMC-B-PIN	OE.AK.sichere_TI	OE.AK.Fachdienste	OE.AK.Admin_EVG	OE.AK.Admin_Konsole	OE.AK.Clientsystem	OE.AK.ClientsystemKorrekt	OE.AK.SW-Update	OE.AK.gSMC-K	OE.AK.Benutzer_Signatur	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro
T.AK.DTBS	X					X	X																X		
T.AK.VAD	X					X	X																		
T.AK.LAN.eHKT	X																								
T.AK.LAN.CS																			X						
T.AK.WAN.TI															X										

	OE.AK.Kartenterminal	OE.AK.Plattform	OE.AK.phys_Schutz	OE.AK.SecAuthData	OE.AK.Personal	OE.AK.HBA	OE.AK.SMC	OE.AK.eGK	OE.AK.Karten	OE.AK.PKI	OE.AK.Echtzeituhr	OE.AK.Versicherter	OE.AK.HBA-Inhaber	OE.AK.SMC-B-PIN	OE.AK.sichere_TI	OE.AK.Fachdienste	OE.AK.Admin_EVG	OE.AK.Admin_Konsole	OE.AK.Clientsystem	OE.AK.ClientsystemKorrekt	OE.AK.SW-Update	OE.AK.gSMC-K	OE.AK.Benutzer_Signatur	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro
T.AK.LAN.Admin																									
T.AK.Kanal_Missbrauch	X														X				X			X			
T.AK.Mani.EVG		X	X								X										X			X	X
T.AK.Mani.Client											X								X					X	X
T.AK.Mani.TI											X				X									X	X
T.AK.Mani.ExternerDienst										X	X													X	X
T.AK.Mani.Chipkarte						X	X	X	X	X	X											X		X	X
T.AK.Mani.Terminal	X									X	X						X							X	X
T.AK.Mani.AdminKonsole											X							X						X	X
T.AK.MissbrauchKarte				X						X	X	X	X	X										X	X
T.AK.Fehlbedienung					X								X				X			X			X		
OSP.AK.MedSoc_Data						X	X															X	X		
OSP.AK.Konn_Spez										X	X													X	X
OSP.AK.KryptAlgo	X					X	X	X							X				X						
OSP.AK.SW-Update											X										X			X	X
OSP.AK.EVG_Modification		X	X		X						X													X	X
OSP.AK.SC_Sign																									
OSP.AK.SC_Authorized						X	X																		
OSP.AK.SC_SVAD	X					X	X																		
OSP.AK.SC_UnalteredData																									
OSP.AK.SV_Certificate										X															
OSP.AK.SV_Signatory																									
OSP.AK.SV_Unaltered_Data																									
OSP.AK.Encryption										X															
OSP.AK.CardService										X															
OSP.AK.Fachanwendungen																X									
OSP.AK.VAUSGD																X									
A.AK.Cardterminal_eHealth	X																								
A.AK.Konnektor		X																							
A.AK.Versicherter												X													
A.AK.HBA-Inhaber													X												
A.AK.SMC-B-PIN														X											
A.AK.sichere_TI															X										
A.AK.Admin_EVG																	X								

	OE.AK.Kartenterminal	OE.AK.Plattform	OE.AK.phys_Schutz	OE.AK.SecAuthData	OE.AK.Personal	OE.AK.HBA	OE.AK.SMC	OE.AK.eGK	OE.AK.Karten	OE.AK.PKI	OE.AK.Echtzeituhr	OE.AK.Versicherter	OE.AK.HBA-Inhaber	OE.AK.SMC-B-PIN	OE.AK.sichere_TI	OE.AK.Fachdienste	OE.AK.Admin_EVG	OE.AK.Admin_Konsole	OE.AK.Clientsystem	OE.AK.ClientsystemKorrekt	OE.AK.SW-Update	OE.AK.gSMC-K	OE.AK.Benutzer_Signatur	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro
A.AK.Env_Arbeitsplatz																			X	X					
A.AK.phys_Schutz			X																						
A.AK.Chipkarteninhaber				X	X																				
A.AK.QSCD						X																			
A.AK.SMC							X																		
A.AK.Benutzer_Signatur																							X		
A.AK.gSMC-K																						X			

Tabelle 13: Abbildung der Sicherheitsziele der Umgebung auf Bedrohungen, OSPs und Annahmen

4.5.3. Detaillierte Erklärung für den Netzkonnektor

4.5.3.1. Bedrohungen gegen den Netzkonnektor

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 11 auf die Bedrohungen abgebildeten Sicherheitsziele geeignet sind, um die Bedrohungen abzuwehren.

T.NK.local_EVG_LAN

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

Optional kann auch O.NK.Stateful bei der Abwehr von T.NK.local_EVG_LAN unterstützen, indem sicherheitsrelevante Ereignisse protokolliert werden. Siehe auch Anwendungshinweis 72:.

T.NK.remote_EVG_WAN

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

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

T.NK.remote_EVG_LAN

Angriffe aus dem Transportnetz werden durch die VPN-Tunnel und den Paketfilter mit Stateful Packet Inspection (zustandsgesteuerte Filterung) abgewehrt: Anfragen, die ein Angreifer aus dem Transportnetz durch einen VPN-Tunnel zu senden versucht, werden vom EVG als ungültig erkannt (weil der Angreifer die VPN-Schlüssel nicht kennt, O.NK.VPN_Integrität) und verworfen. Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die Inhalte, die durch den VPN-Tunnel mit der zentralen TI-Plattform übertragen werden, sind nicht bösartig (OE.NK.sichere_TI). Anfragen außerhalb des VPN-Tunnels werden durch den dynamischen Paketfilter gefiltert (O.NK.PF_WAN); der EVG schützt durch diesen WAN-seitigen Paketfilter sich selbst und weitere dezentrale Komponenten im LAN der Leistungserbringer. Der WAN-seitige Paketfilter bietet zustandsgesteuerte Filterung (stateful packet inspection, zustandsgesteuerte Filterung, O.NK.Stateful). Der dynamische Paketfilter wird dabei unterstützt von O.NK.Protokoll, indem sicherheitsrelevante Ereignisse mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) protokolliert werden. Konnte ein Clientsystem bereits kompromittiert werden, so unterstützt auch der LAN-

seitige Paketfilter beim Schutz des EVG (O.NK.PF_LAN): Im Fall einer Einbox-Lösung schützt der EVG (O.NK.PF_LAN) auch den Anwendungskonnektor vor LAN-seitigen Angriffen und trägt somit zur Abwehr der Bedrohung bei. Der EVG wird – wie bei T.NK.remote_EVG_WAN – unterstützt von O.NK.Schutz, indem Selbsttests durchgeführt werden, die Veränderungen der Integrität des EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

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

Angriffe aus dem Internet über den VPN-Tunnel vom Sicheren Internet Service (siehe Angriffspfad 3.2 in Abbildung 2) werden durch die Sicherheitsfunktionalität des Sicheren Internet Service verhindert (OE.NK.SIS). Entsprechende Zugriffe werden dadurch erkannt und vor der Weiterleitung über den VPN-Tunnel zum EVG blockiert. Zusätzlich kann der LAN-seitige Paketfilter (O.NK.PF_LAN) zum Schutz des LAN und des EVG beitragen. Konnte ein LAN dennoch kompromittiert werden, schützen die LAN-seitig installierten Maßnahmen zur Erkennung und Schutz vor bösartigem Code (OE.NK.Betrieb_CS) die Clientsysteme und den EVG.

Optional kann auch O.NK.Stateful bei der Abwehr von T.NK.remote_EVG_LAN unterstützen, indem sicherheitsrelevante Ereignisse nicht nur – wie bei T.NK.remote_EVG_WAN – an der WAN-seitigen Schnittstelle, sondern auch an der LAN-seitigen Schnittstelle protokolliert werden (Schreiben von Audit-Daten zur späteren Auswertung mit dem Ziel zustandsgesteuerter Filterung). Siehe auch Anwendungshinweis 72:.

T.NK.remote_VPN_Data

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

Mit den gleichen Argumenten wie bei T.NK.remote_EVG_WAN (der Aufbau des sicheren Kanals wird vorab durch eine gegenseitige Authentisierung geschützt, die wiederum eine Zertifikatsgültigkeitsprüfung und eine Überprüfung der Systemzeit umfasst), tragen auch die

Ziele O.NK.VPN_Auth, O.NK.Zert_Prüf, OE.NK.PKI, O.NK.Zeitdienst, OE.NK.Zeitsynchro, OE.NK.KeyStorage, OE.NK.Ersatzverfahren und OE.NK.RNG zur Abwehr der Bedrohung bei.

Anwendungshinweis 73: O.NK.Protokoll (Sicherheits-Log) wird im ST nicht bei der Abwehr von T.NK.remote_VPN_Data berücksichtigt. Siehe auch Anwendungshinweis 72:.

T.NK.local_admin_LAN

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

Anwendungshinweis 74: Im Rahmen der Administration kommen kryptographische Verfahren zum Einsatz (Implementierung eines sicheren Kanals). Damit trägt auch OE.NK.Ersatzverfahren zur Abwehr von T.NK.local_admin_LAN und T.NK.remote_admin_WAN bei. OE.NK.phys_Schutz trägt zur Abwehr von T.NK.local_admin_LAN beitragen, da durch den Schutz des Kommunikationskanals zwischen dem EVG und weiteren Komponenten des Konnektors Manipulationen am Gerät verhindert werden können. Siehe auch Anwendungshinweis 72: (Anpassung des Security Targets bei Bedarf).

T.NK.remote_admin_WAN

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

O.NK.Admin_Auth, OE.NK.Admin_EVG, OE.NK.RNG, O.NK.Protokoll, O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, O.NK.Schutz und OE.NK.KeyStorage bei. Für die Administration wird ein sicherer TLS Kanal aufgebaut. Hinsichtlich der dabei verwendeten kryptographischen Verfahren trägt OE.NK.Ersatzverfahren zur Abwehr von T.NK.remote_admin_WAN bei.

T.NK.counterfeit

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

T.NK.Zert_Prüf

Bei der Bedrohung T.NK.Zert_Prüf manipuliert ein Angreifer Sperrlisten, die zum Zwecke der Gültigkeitsprüfung von Zertifikaten von einem netzbasierten Dienst verteilt werden. Dieser Angriff wird durch das Ziel O.NK.Zert_Prüf auf Basis der über OE.NK.PKI erhaltenen Informationen abgewehrt. Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der bei den Zertifikaten genutzten kryptographischen Algorithmen richten. Im Rahmen der Gültigkeitsprüfung von Zertifikaten werden Plausibilitätsprüfungen durchgeführt, welche die Echtzeit des EVG verwenden; somit trägt auch O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro zur Abwehr von T.NK.Zert_Prüf bei. Zudem trägt auch O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr von T.NK.Zert_Prüf bei, da fehlgeschlagene oder erfolgreiche Updates der Sperrlisten protokolliert werden. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der gSMC-K gespeichert sind, daher unterstützt OE.NK.gSMC-K bei der Abwehr von T.NK.Zert_Prüf. Ein externer Zufallszahlengenerator (OE.NK.RNG) wird darüber hinaus als Lieferant für gute Zufallszahlen genutzt, die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen.

Anwendungshinweis 75: .O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, O.NK.Protokoll, OE.NK.gSMC-K, OE.NK.RNG, O.NK.PF_WAN und entsprechend O.NK.Stateful tragen zur Abwehr von T.NK.Zert_Prüf bei.

T.NK.TimeSync

T.NK.TimeSync beschreibt den Angriff, dass Nachrichten manipuliert werden, die im Rahmen einer Zeitsynchronisation mit einem netzbasierten Dienst ausgetauscht werden, um auf dem EVG die Einstellung einer falschen Echtzeit zu bewirken. Dieser Angriff wird durch das Ziel O.NK.Zeitdienst abgewehrt, da dieses die Synchronisation der durch die Umgebung

bereitgestellte Echtzeituhr (OE.NK.Echtzeituhr) über einen sicheren Kanal fordert. Weil der Zeitdienst innerhalb der zentralen Telematikinfrastruktur-Plattform bereitgestellt wird, dient bereits der VPN-Tunnel zu dem VPN-Konzentrator für den Zugang zur Telematikinfrastruktur als sicherer Kanal (O.NK.VPN_Integrität). Die gSMC-K speichert das für den VPN-Kanal erforderliche Schlüsselmaterial (OE.NK.gSMC-K). Die gSMC-K kann darüber hinaus als Lieferant für gute Zufallszahlen genutzt werden (OE.NK.RNG), die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Beim Aufbau des Kanals werden die Kummunikationspartner authentisiert (O.NK.VPN_Auth) und Zertifikat geprüft (O.NK.Zert_Prüf) gegen die PKI der TI (OE.NK.PKI). Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der beim VPN-Kanal genutzten kryptographischen Algorithmen richten. Die Zeitserver, die über eine verlässliche Systemzeit verfügen und somit die Basis für eine vertrauenswürdige Zeitinformation im Rahmen der Synchronisierung bilden, werden durch die Umgebung bereitgestellt (OE.NK.Zeitsynchro); außerdem liegen sie innerhalb der Telematikinfrastruktur und bilden somit die Gegenseite des sicheren Kanals. Zudem trägt O.NK.Protokoll zur Abwehr der Bedrohungen bei, da erfolgreiche oder fehlgeschlagene Zeitsynchronisation protokolliert wird.

Anwendungshinweis 76: O.NK.Protokoll, OE.NK.gSMC-K, OE.NK.RNG, OE.NK.PKI und OE.NK.Ersatzverfahren tragen zur Abwehr von T.NK.TimeSync bei.

T.NK.DNS

Die Bedrohung T.NK.DNS beschreibt einen Angriff aus dem Transportnetz, bei dem Antworten auf DNS-Anfragen gefälscht werden. Solche DNS-Anfragen an DNS-Server im Transportnetz bzw. im Internet kommen nur in solchen Szenarien vor, bei denen Adressen im Transportnetz bzw. Internet aufgelöst werden sollen[25]. Der Netzkonnektor löst die öffentlichen Adressen der VPN-Konzentratoren mittels DNS-Anfragen auf. Bei erfolgtem Angriff bekommt er nicht die gewünschte Adresse zurück. Das führt aber dazu, dass er keinen VPN-Kanal aufbauen kann, da durch das Sicherheitsziel O.NK.VPN_Auth die Authentisierung der VPN-Konzentratoren erforderlich ist. Dabei findet eine Zertifikatsprüfung statt (O.NK.Zert_Prüf) gegen die PKI der TI (OE.NK.PKI). Sichere Ersatzverfahren (OE.NK.Ersatzverfahren) unterstützen bei der Abwehr von Angriffen, die sich gegen Schwächen der bei den Zertifikaten genutzten kryptographischen Algorithmen richten. Damit erlangt der Angreifer keinen Zugriff auf das LAN des Leistungserbringers und kann die zu schützenden Daten nicht angreifen. Bei versuchtem Angriff kann dieser unter Umständen durch den Paketfilter des Netzkonnektors erkannt und verhindert werden (O.NK.PF_WAN, O.NK.Stateful). Dies hängt einerseits vom Vorgehen des Angreifers und andererseits von der Funktionalität des Paketfilters ab. Bei erkanntem Angriff erfolgt ferner ein Eintrag mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) in das Sicherheitsprotokoll (O.NK.Protokoll).

Im Fall einer DNS-Auflösung durch Clientsysteme beim Zugriff auf das Internet führt die Manipulation der DNS-Antwort dazu, dass Clientsysteme auf Seiten umgelenkt werden können, die nicht ihrer ursprünglichen Intention entsprechen. Erfolgt dies vom Benutzer unbemerkt, können bei bösartigen Systemen die Clientsysteme durch bösartigen Code infiziert

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

werden. Dies kann einerseits durch Erkennungsmechanismen im SIS verhindert werden, welches wirksame Maßnahmen gegen Angriffe aus dem Internet implementieren soll (OE.NK.SIS). In jedem Fall muss der bösartige Code auf den Clientsystemen aber durch Mechanismen auf den Clientsystemen (Einsatz von sicheren Produkten und Virenscannern) erkannt und neutralisiert werden (OE.NK.Betrieb_CS).

4.5.3.2. Organisatorische Sicherheitspolitiken für den Netzkonnektor

OSP.NK.Zeitdienst

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

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

OSP.NK.SIS

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

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

OSP.NK.BOF

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

OSP.NK.TLS

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

OSP.NK.SW-Update

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

4.5.3.3. Annahmen des Netzkonnektors

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

Die Annahme A.NK.Zugriff_gSMC-K lautet:

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

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

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

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

4.5.4. Detaillierte Erklärung für den Anwendungskonnektor

4.5.4.1. Bedrohungen

T.AK.DTBS

Die Bedrohung T.AK.DTBS beschreibt Angriffe, bei denen der Angreifer erfolgreich Daten ohne die oder entgegen der Intention des Signaturschlüssel-Inhabers durch die sichere Signaturerstellungseinheit oder andere Chipkarten signieren lassen kann. Mit OE.AK.Benutzer_Signatur ist sichergestellt, dass der Benutzer des Clientsystems vor Übermittlung an den EVG verifiziert hat, dass die an den EVG zur Signierung übermittelten Daten mit den intendierten Daten übereinstimmen. Gemäß O.AK.Sig.exklusivZugriff bereitet der EVG die vom Benutzer des Clientsystems autorisierten, zu signierenden Daten für die Signaturerstellung durch die QSEE vor, sorgt für den alleinigen Zugriff auf die QSEE, sendet sie an die QSEE (der HBA gemäß OE.AK.HBA, im Falle nichtqualifizierter elektronischer Signaturen die SMC-B gemäß OE.AK.SMC), und kontrolliert die empfangenen Signaturen und vergleicht die signierten mit den autorisierten Daten. Zusätzlich wird die Kommunikation zwischen AK und den eHealth-Kartenterminals, in denen die Chipkarten (einschließlich QSEE) stecken, gemäß O.AK.IFD-Komm geschützt. Die TLS-Kanäle werden durch die eHealth-Kartenterminals gemäß OE.AK.Kartenterminal unterstützt.

T.AK.VAD

Die Bedrohung T.AK.VAD beschreibt Angriffe, über das lokale Netz die VAD (d.h. die PIN oder PUK) eines Chipkartenbenutzers zu kompromittieren oder zu manipulieren. Die Benutzerauthentisierung gegenüber Chipkarten wird durch O.AK.VAD bei lokaler und entfernter PIN-Eingabe direkt geschützt. Die Vertraulichkeit und der Integritätsschutz der VAD bei der entfernten PIN-Eingabe werden durch Secure Messaging Kanäle zwischen der gSMC-K in den PIN-Terminals und den Chipkarten HBA und SMC-B erreicht, welche gemäß O.AK.VAD durch den EVG gesteuert und gemäß OE.AK.HBA und OE.AK.SMC von allen benutzten Chipkarten unterstützt wird. Die Vertraulichkeit und Integrität der VAD wird in den eHealth-Kartenterminals gemäß OE.AK.Kartenterminal geschützt. Die Vertraulichkeit und Integrität der Kommunikation zwischen PIN-Terminal und Chipkarten-Terminal wird zusätzlich durch entsprechend gesicherte Kanäle gemäß O.AK.IFD-Komm und OE.AK.Kartenterminal geschützt.

T.AK.LAN.eHKT

Die Bedrohung T.AK.LAN.eHKT wird direkt durch das EVG-Sicherheitsziel O.AK.IFD-Komm unter den Bedingungen des Sicherheitsziels der Einsatzumgebung OE.AK.Kartenterminal abgedeckt. O.AK.Admin gewährleistet die Administration der eHealth-Kartenterminals durch Administratoren.

T.AK.LAN.CS

Die Bedrohung T.AK.LAN.CS beschreibt Angriffe auf die Integrität und Vertraulichkeit der im LAN zwischen dem EVG und Clientsystemen übertragenen Daten. Das Sicherheitsziel O.AK.LAN schützt gegen Abhören, Fälschen und Vorgeben einer falschen Identität bei der Kommunikation mit den Clientsystemen im LAN der Leistungserbringer. Bei der Gegenstelle

der Kommunikation ist ein ebenso vertrauenswürdiger Umgang mit den übertragenen Daten und mit dem genutzten Schlüsselmaterial erforderlich. Dies wird mit dem Sicherheitsziel OE.AK.Clientsystem erreicht.

T.AK.WAN.TI

Bei der Bedrohung T.AK.WAN.TI werden Daten bei der Übertragung zwischen EVG und Fachdiensten abgehört oder manipuliert. Diese Bedrohung wird seitens des EVG direkt durch das Sicherheitsziel O.AK.WAN adressiert. Bei der Gegenstelle der Kommunikation ist ein ebenso vertrauenswürdiger Umgang mit den übertragenen Daten und mit dem genutzten Schlüsselmaterial erforderlich. Dies wird mit dem Sicherheitsziel OE.AK.sichere_TI erreicht.

T.AK.LAN.Admin

Die Bedrohung T.AK.LAN.Admin betrachtet Angriffe auf die Kommunikation zwischen Adminstrationskonsole und EVG. Das Sicherheitsziel O.AK.Admin fordert dafür eine bezüglich Integrität und Vertraulichkeit gesicherte Kommunikation, um diese Bedrohung abzudecken.

T.AK.Kanal_Missbrauch

Bei der Bedrohung T.AK.Kanal_Missbrauch werden bestehende (logische) Kommunikationskanäle durch Angreifer missbraucht. Dies wird durch folgende Maßnahmen adressiert:

- Das Sicherheitsziel O.AK.Admin verhindert durch den Schutz der Integrität und Vertraulichkeit des Kommunikationskanals zur Administrationsschnittstelle, dass zusätzliche Daten eingeschleust werden können oder eine bestehende Kommunikation modifiziert werden kann.
- Das Sicherheitsziel der Umgebung OE.AK.gSMC-K verhindert durch den Schutz der Integrität und Vertraulichkeit des Kommunikationskanals zwischen EVG und gSMC-K, dass zusätzliche Daten eingeschleust werden können oder eine bestehende Kommunikation modifiziert werden kann.
- Das Sicherheitsziel O.AK.IFD-Komm verhindert durch den Schutz der Integrität und Vertraulichkeit der Kommunikation zwischen EVG und eHealth-Terminal, dass zusätzliche Daten eingeschleust werden können oder eine bestehende Kommunikation modifiziert werden kann. Für die Gegenstelle der Kommunikation (eHealth-Kartenterminal) wird entsprechendes in den Sicherheitszielen für die Umgebung OE.AK.Kartenterminal gefordert.
- Das Sicherheitsziel O.AK.Sig.exklusivZugriff fordert die Überwachung der Integrität der zum Signieren vom EVG an die QSEE übergebenen Daten. Zudem wird die alleinige Kontrolle über die QSEE durch den autorisierten Nutzer sichergestellt. Damit wird ein Missbrauch des Kanals zur QSEE verhindert.
- Bei der Kommunikation zwischen EVG und Clientsystem bzw. zwischen EVG und Fachanwendungen in der zentralen TI-Plattform werden bezüglich Integrität und Vertraulichkeit gesicherte Kanäle verwendet. Dies ist durch die Sicherheitsziele O.AK.LAN und O.AK.WAN für den EVG realisiert, für die Gegenstellen der

Kommunikation wird entsprechendes in den Sicherheitszielen für die Umgebung OE.AK.sichere_TI und OE.AK.Clientsystem gefordert.

- Für die Kommunikation zwischen EVG und Kartenterminal bzw. zwischen EVG und Chipkarte fordert das Sicherheitsziel O.AK.exklusivZugriff die alleinige Kontrolle des Benutzers über diese Instanzen. Die genutzten Ressourcen werden nach Beendigung der Transaktion wieder freigegeben. Damit wird ein Missbrauch der entsprechenden Kommunikationskanäle verhindert.

T.AK.Mani.EVG

Die Bedrohung T.AK.Mani.EVG betrachtet Manipulationen des EVG durch direkten Zugriff auf den EVG oder auf Update-Daten. Das Sicherheitsziel für die Umgebung OE.AK.phys_Schutz schützt den EVG vor Manipulationen und physischen Zugriff durch Unbefugte. Zusätzlich bietet die Plattform (Ausführungsumgebung) des EVG einen Schutz durch OE.AK.Plattform. Das Sicherheitsziel O.AK.EVG_Modifikation adressiert logische Bedrohungen auf sicherheitsrelevante Anteile zur Laufzeit des EVG und sorgt für Erkennung von Modifikationen und den Schutz kryptografischer Geheimnisse. Erkannte Veränderungen führen zu einem entsprechenden Betriebszustand des EVG, der stets den sicheren Zustand des EVG aufrecht erhält. Solche Veränderungen werden durch O.AK.Protokoll sicher protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen. Unautorisierte Veränderungen von Update-Daten werden durch OE.AK.SW-Update verhindert und manipulierte Update-Daten werden durch O.AK.Update erkannt und nicht angewendet. O.AK.Selbsttest stellt Fehler fest, die ggf. durch Manipulationen hervorgerufen werden.

T.AK.Mani.Client

Die Bedrohung T.AK.Mani.Client betrachtet manipulierte Clientsysteme, um zu schützende Daten offenzulegen oder zu manipulieren. Im Sicherheitsziel OE.AK.Clientsystem werden vertrauenswürdige Clientsysteme gefordert, von denen keine Angriffe ausgehen und die mit zu schützenden Daten und mit Schlüsselmaterial entsprechend sorgsam umgehen. Falls dennoch sicherheitskritische Ereignisse durch manipulierte Clientsysteme im EVG festgestellt werden, so werden diese durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen. Erfolgreich manipulierte Clientsysteme können zu einer Verletzung der spezifizierten Abläufe im EVG gemäß Informationsmodell führen. Diese Verletzungen werden durch das Sicherheitsziel O.AK.Infomodell wirksam verhindert.

T.AK.Mani.TI

Die Bedrohung T.AK.Mani.TI betrachtet Angriffe durch manipulierte Systeme in der zentralen TI-Plattform. Dies wird durch OE.AK.sichere_TI wirksam verhindert, indem es eine vertrauenswürdige TI fordert, von der keine Angriffe ausgehen und die zu schützende Daten nicht missbraucht. Angriffe durch Administratoren der TI werden ebenso ausgeschlossen wie Bedrohungen durch fehlerhafte Software. Falls dennoch sicherheitskritische Ereignisse durch manipulierte Systeme der zentralen TI-Plattform im EVG festgestellt werden, so werden diese durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.Mani.ExternerDienst

Die Bedrohung T.AK.Mani.ExternerDienst betrachtet den Einfluss externer Dienste (dem PKI-Dienst), die zur ordnungsgemäßen Funktion des EVG benötigt werden. Im Fall von PKI-Diensten fordert das Sicherheitsziel OE.AK.PKI den Zugriff auf alle notwendigen Informationen zur Prüfung von Zertifikaten durch den EVG. Die öffentlichen Schlüssel der Wurzelinstanzen werden auf vertrauenswürdige Weise zur Verfügung gestellt. Dadurch werden Modifikationen an bzw. mit Hilfe des PKI Dienstes zuverlässig vom EVG erkannt und durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.Mani.Chipkarte

Manipulierte Chipkarten werden durch die Bedrohung T.AK.Mani.Chipkarte betrachtet. Die eingesetzten Chipkarten sind gemäß OE.AK.SMC, OE.AK.HBA, OE.AK.eGK evaluiert und zertifiziert und verfügen somit über entsprechende Schutzmechanismen, die Manipulationen wirksam verhindern. Gemäß OE.AK.Karten werden gefälschte Chipkarten in Kartenlesern des LAN des Leistungserbringers erkannt bzw. die Verarbeitung ungesicherter persönlicher Daten der Chipkarten verhindert. Die gSMC-K ist durch die gematik zugelassen und verfügt damit ebenfalls über entsprechende Schutzmechanismen (OE.AK.gSMC-K). Der EVG bietet mit der Nutzung einer PKI (OE.AK.PKI) Möglichkeiten zum Zurückziehen von Kartenzertifikaten, die eine weitere Nutzung der betroffenen Identitäten auf den Chipkarten verhindern. Dies wird insbesondere durch die Sicherheitsziele O.AK.Update und O.AK.Infomodell erreicht: Durch O.AK.Update werden dem EVG entsprechende Listen über den Status von Identitäten geliefert, die für die Zuordnung der einzelnen Komponenten im Betrieb des EVG im Sinne des Informationsmodells benötigt werden. Abweichungen vom Informationsmodell werden durch O.AK.Infomodell nicht akzeptiert, durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.Mani.Terminal

Die Bedrohung T.AK.Mani.Terminal adressiert manipulierte eHealth-Terminals, um unautorisierten Zugriff auf zu schützende Daten zu erlangen. Das Sicherheitsziel OE.AK.Kartenterminal verlangt den Einsatz von sicheren Kartenterminals, die implementierte Sicherheitsmechanismen sicherstellen, welche für den Betrieb des EVG benötigt werden. Da diese Terminals über Chipkarten (gSMC-KT) verfügen, sind ihre Identitäten durch die PKI-Dienste im EVG (siehe OE.AK.PKI) erfasst. Der EVG setzt das Informationsmodell gemäß O.AK.Infomodell durch, das beim Pairing der Komponenten durch den Administrator konfiguriert werden kann. Nur vertrauenswürdige Komponenten werden durch den Administrator im Informationsmodell implementiert (OE.AK.Admin_EVG). Durch die Nutzung der PKI (OE.AK.PKI, O.AK.Update) werden nicht vertrauenswürdige Terminals von der Nutzung ausgeschlossen. Unautorisierte Zugriffsversuche solcher Terminals widersprechen dem Informationsmodell (O.AK.Infomodell) und werden durch den EVG ausgeschlossen, protokolliert (O.AK.Protokoll) und mit einem sicheren Zeitstempel versehen (O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro)).

T.AK.Mani.AdminKonsole

Die Bedrohung T.AK.Mani.AdminKonsole betrachtet manipulierte Administrationskonsolen, um unautorisiert Veränderungen am EVG vorzunehmen oder Zugriff auf zu schützende Daten zu erlangen. Die wird durch OE.AK.Admin_Konsole verhindert, wobei eine sichere Administrationskonsole gefordert wird. Zudem fordert das Sicherheitsziel O.AK.Admin entsprechende Mechanismen, die nur erfolgreich authentisierten Administratoren Zugriff zu administrativen Funktionen des EVG erlauben. Erkannte Verstöße werden durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.MissbrauchKarte

Die Bedrohung T.AK.MissbrauchKarte betrachtet Gefahren durch missbrauchte Chipkarten im Zusammenhang mit Diebstahl und/oder Nutzung von ausgespähten PINs. Dies wird durch Sorgfaltspflichten der entsprechenden Kartenbesitzer bzw. Nutzer gemäß OE.AK.Versicherter, OE.AK.HBA-Inhaber, OE.AK.SMC-B-PIN sowie OE.AK.SecAuthData verhindert. Sollte trotzdem eine Chipkarte abhanden gekommen sein, so kann durch Einsatz der PKI (OE.AK.PKI , O.AK.Update) die entsprechende Identität gesperrt werden. Der EVG setzt das Informationsmodell gemäß O.AK.Infomodell durch und verhindert so den Einsatz dieser gesperrten Chipkarten. Versuchte Nutzungen solcher Karten werden gemäß O.AK.Protokoll protokolliert und mit einem sicheren Zeitstempel versehen (O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro)). Bei einer festgestellten ausgespähten PIN erlaubt der EVG das Management von PIN-Änderungen durch den Benutzer (O.AK.PinManagement).

T.AK.Fehlbedienung

Die Bedrohung T.AK.Fehlbedienung betrachtet Gefahren durch Fehlkonfiguration oder Fehlbedienung des EVG. Im Fall der Administration des EVG verlangt OE.AK.Admin_EVG, dass Administratoren hinreichend vertrauenswürdig und geschult sind, um Fehlbedienungen zu verhindern. Für Benutzer des EVG über Clientsysteme hängt die Gefahr der Fehlbedienung auch von der korrekten Gestaltung der Benutzerschnittstelle und der Software der Clientsysteme ab. Hierzu fordert zum einen OE.AK.ClientsystemKorrekt die korrekte Implementierung der Clientsysteme entsprechend dem Informationsmodell sowie eine korrekte und verständliche Darstellung von Meldungen, Warnungen und kritischen Betriebszuständen. Zum anderen fordert OE.AK.Personal, dass das Personal so qualifiziert ist, dass Fehler bei Betrieb und Nutzung des EVG ausgeschlossen sind. Das minimiert die Gefahr von Fehlbedienungen an dieser Schnittstelle. Sorgfaltspflichten des Benutzers bzw. HBA-Inhabers tragen gemäß OE.AK.Benutzer_Signatur bzw. OE.AK.HBA-Inhaber zur Vermeidung von Fehlbedienungen bei.

4.5.4.2. Organisatorische Sicherheitspolitiken

OSP.AK.MedSoc_Data

Die Sicherheitspolitik OSP.AK.MedSoc_Data verlangt, Dienste zur qualifizierten und nichtqualifizierten elektronischen Signatur, zur Chiffrierung von Dateien sowie zur

kryptographischen Absicherung der Kommunikation bereitzustellen. Dadurch wird die Vertraulichkeit und Integrität aller Daten, die durch oder an die Telematikinfrastruktur, ein Clientsystem des Leistungserbringers oder eine elektronische Gesundheitskarte übergeben werden, gewährleistet. Die Sicherheitsziele des EVG tragen dem wie folgt Rechnung:

- O.AK.Sig.SignNonQES, O.AK.Sig.Stapelsignatur O.AK.Sig.Komfortsignatur und O.AK.Sig.SignQES fordern die Bereitstellung von Signaturdiensten für die Erstellung nichtqualifizierter elektronischer Signaturen mit der SMC-B (s.OE.AK.SMC) qualifizierter elektronischer Signaturen mit dem HBA als QSEE (s. OE.AK.HBA),
- O.AK.Sig.PrüfungZertifikat, O.AK.Sig.Schlüsselinhaber und O.AK.Sig.SignaturVerifizierung fordern die Dienste zur Signaturprüfung,
- OE.AK.Benutzer_Signatur fordert den Benutzer des Clientsystems zur Überprüfung der zu signierenden Daten vor Übermittlung an den EVG auf
- O.AK.Enc und O.AK.Dec stellen die Verschlüsselung und Entschlüsselung von Dokumenten für die Übermittlung in die Telematikinfrastruktur bereit,
- O.AK.IFD-Komm schützt die durch den EVG erzeugte Kommunikation im LAN des Leistungserbringers,
- O.AK.LAN, O.AK.WAN und OE.AK.gSMC-K schützen Integrität und Vertraulichkeit bei der Kommunikation des EVG mit Clientsystemen, mit Fachdiensten und mit der gSMC-K.
- O.AK.exklusivZugriff verhindert den Zugriff auf eine aktive Sitzung (Session) zwischen EVG und Kartenterminal bzw. zwischen EVG und Chipkarte durch unautorisierte Instanzen.
- Der EVG implementiert das Infomodell gemäß O.AK.Infomodell und stellt damit sicher, dass spezifizierten Abläufe und Zuordnungen der Komponenten im Betrieb eingehalten werden.

OSP.AK.Konn_Spez

Die Sicherheitspolitik OSP.AK.Konn_Spez fordert die Erfüllung der sicherheitsrelevanten Anforderungen der Konnektor-Spezifikation [27] und die Durchsetzung der zulässigen Signaturrichtlinien und Verschlüsselungsrichtlinien. Die EVG-Sicherheitsziele O.AK.Admin, O.AK.IFD-Komm, (Kommunikation mit eHealth-Kartenterminals), O.AK.Enc, O.AK.Dec, O.AK.Sig.SignQES, O.AK.Sig.Einfachsignatur, O.AK.Sig.Stapelsignatur, O.AK.Sig.Komfortsignatur, O.AK.Protokoll, O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro), O.AK.Update sowie bezüglich der Verwendung von Chipkarten O.AK.VAD, O.AK.exklusivZugriff und O.AK.PinManagement setzen Spezifikationsanteile von [27] um (und andere EVG-Sicherheitsziele präzisieren diese). Die Durchsetzung zulässiger Signaturrichtlinien wird explizit in O.AK.Sig.SignQES und für Verschlüsselungsrichtlinien in O.AK.Enc gefordert, deren Bereitstellung durch OE.AK.PKI gewährleistet wird. Das Sicherheitsziel OE.AK.Echtzeituhr (mit Hilfe von O.NK.Zeitdienst und OE.NK.Echtzeituhr) deckt die Anforderungen der Konnektor-Spezifikation zur Verwendung von Echtzeit ab. Die spezifizierten Abläufe und Zuordnungen zwischen dem EVG und externen Komponenten werden durch O.AK.Infomodell im EVG implementiert.

OSP.AK.KryptAlgo

Die Sicherheitspolitik OSP.AK.KryptAlgo fordert den Einsatz kryptografischer Verfahren im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 und wird im EVG direkt durch das Sicherheitsziel O.AK.Basis_Krypto umgesetzt. Außerhalb des EVG wird diese Sicherheitspolitik durch entsprechende Sicherheitsziele für die Umgebung durchgesetzt: OE.AK.sichere_TI fordert die Verwendung von kryptographischen Sicherheitsmechanismen, die Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 implementiert sind. Gleiches fordert OE.AK.Clientsystem für die Clientsysteme. Im Fall der Kartenterminals und Chipkarten wird die Sicherheitspolitik durch den Einsatz entsprechend zertifizierter Komponenten sichergestellt. Dies drückt sich in den Sicherheitszielen für die Einsatzumgebung OE.AK.Kartenterminal, OE.AK.HBA, OE.AK.SMC und OE.AK.eGK aus.

OSP.AK.SW-Update

Die Sicherheitspolitik OSP.AK.SW-Update erlaubt das Einspielen von Software für Konnektorkomponenten im Sinne einer Aktualisierung sowie das Aktualisieren der TSF Daten und das Nachladen von Fachmodulen. Der Admin kann konfigurieren, dass die Aktualisierung automatisch stattfindet oder der Admin kann die Aktualisierung manuell anstoßen. Die Änderung der Konfiguration zum automatischen Update und das manuelle Anwenden von Aktualisierungen ist ein administrativer Vorgang und damit auf Personen mit administrativen Zugriffsrechten beschränkt. Dies wird durch das Sicherheitsziel O.AK.Admin erreicht. In diesem Zusammenhang stehende sicherheitsrelevante Ereignisse werden durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (sowie OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen. Bei der Bereitstellung der Update-Daten sorgt die Einsatzumgebung gemäß OE.AK.SW-Update dafür, dass nur geprüfte und von einer autorisierten Stelle freigegebene und ggf. zertifizierte SW-Updates signiert und bereitgestellt werden. Ebenso sorgt OE.AK.SW-Update dafür, dass nur geprüfte und von einer autorisierten Stelle freigegebene Fachmodule signiert und ausgeliefert werden. Zum Software-Update im EVG fordert O.AK.Update, dass nur solche Updates eingespielt werden dürfen, deren Integrität und Authentizität gesichert ist.

OSP.AK.EVG_Modification

Die Sicherheitspolitik OSP.AK.EVG_Modification wird durch das EVG-Sicherheitsziel

- O.AK.EVG_Modifikation zur Erkennbarkeit logischer Angriffe auf den EVG
- O.AK.Protokoll für eine Protokollierung mit einem sicheren Zeitstempel (O.AK.Zeit, OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro)

und unter den Bedingungen der Sicherheitsziele für die Einsatzumgebung

- OE.AK.Personal zur Kontrolle durch das Personal, ob der EVG sicherheitstechnische Veränderungen erkennen lässt,
- OE.AK.phys_Schutz zum physischen Schutz des EVG,
- OE.AK.Plattform zur vertrauenswürdigen Plattform zur Ausführung des EVG

geeignet umgesetzt.

OSP.AK.SC_Sign

Die Sicherheitspolitik OSP.AK.SC_Sign zur Erstellung qualifizierter elektronische Signaturen mit dem HBA als QSEE und digitaler Signaturen mit anderen Chipkarten als Signaturerstellungseinheit und dem EVG wird durch die folgenden EVG-Sicherheitsziele umgesetzt:

- O.AK.Sig.SignQES, O.AK.Sig.Einfachsignatur, O.AK.Sig.Komfortsignatur und O.AK.Sig.Stapelsignatur fordern die Erstellung der in OSP.AK.SC_Sign genannten qualifizierten elektronischen Signaturen in Abhängigkeit von der gewählten Signaturrichtlinie.
- O.AK.Sig.SignNonQES fordert die Erstellung der in OSP.AK.SC_Sign genannten nichtqualifizierten elektronischen Signaturen in Abhängigkeit von der gewählten Signaturrichtlinie sowie die Erzeugung digitaler Signaturen über Bitstrings mit Authentisierungsschlüsseln.

OSP.AK.SC_Authorized

Die Sicherheitspolitik OSP.AK.SC_Authorized wird durch Sicherheitsziele für den EVG und der Einsatzumgebung umgesetzt:

- O.AK.Sig.exklusivZugriff fordert, dass der EVG nur für solche Dateien und Heilberufsausweise den Signaturprozess auslösen darf, die von dem autorisierten Benutzer des Clientsystems ausgewählt wurden (Stapel). Die Autorisierung basiert auf einer erfolgreichen Authentisierung des Benutzers des Clientsystems als Signaturschlüssel-Inhaber, die nach OE.AK.HBAund OE.AK.SMC für die Nutzung des Signaturschlüssels notwendig ist. Darüber hinaus prüft der EVG, ob nur die autorisierten zu signierenden Daten korrekt signiert wurden.
- O.AK.VAD schützt die SVAD durch die Eingabe der Signatur-PIN und Signatur-PUK des Signaturschlüssel-Inhabers im sicheren PIN-Modus am PIN-Terminal und deren vertrauliche und integritätsgeschützte Übermittlung im Secure Messaging Kanal zwischen der SMC im PIN-Terminal zur SVAD-empfangenden QSEE im Chipkarten-Terminal. Außerdem sorgt dieses Sicherheitsziel des EVG für die spätere Anzeige der übergebenen Jobnummer am PIN-Terminal.

OSP.AK.SC_SVAD

Die Sicherheitspolitik OSP.AK.SC_SVAD wird durch das EVG-Sicherheitsziel O.AK.VAD und die Sicherheitsziele der anderen beteiligten Komponenten der Einsatzumgebung OE.AK.Kartenterminal, OE.AK.HBA und OE.AK.SMC umgesetzt.

OSP.AK.SC_UnalteredData

Die Sicherheitspolitik OSP.AK.SC_UnalteredData wird durch die Ziele O.AK.Sig.exklusivZugriff, O.AK.Sig.Einfachsignatur, O.AK.Sig.Komfortsignatur und O.AK.Sig.Stapelsignatur umgesetzt.

OSP.AK.SV_Certificate

Die Sicherheitspolitik OSP.AK.SV_Certificate wird durch das EVG-Sicherheitsziel O.AK.Sig.PrüfungZertifikat umgesetzt. Dabei unterstützt die Einsatzumgebung den EVG durch das Sicherheitsziel OE.AK.PKI.

OSP.AK.SV_Signatory

Die Sicherheitspolitik OSP.AK.SV_Signatory wird durch das geeignet formulierte Ziel O.AK.Sig.Schlüsselinhaber umgesetzt.

OSP.AK.SV_Unaltered_Data

Die Sicherheitspolitik OSP.AK.SV_Unaltered_Data wird durch folgende Sicherheitsziele des EVG und der Umgebung umgesetzt:

- O.AK.Sig.SignaturVerifizierung, der vom EVG fordert, zuverlässig die Korrektheit einer qualifizierten elektronischen Signatur und andere digitaler Signaturen und die Unverändertheit der signierten Daten zu prüfen und das Ergebnis der Prüfung zutreffend anzuzeigen.

OSP.AK.Encryption

Die Sicherheitspolitik OSP.AK.Encryption wird durch die EVG-Sicherheitsziele und die Einsatzumgebung umgesetzt:

- O.AK.Enc fordert die Bereitstellung des Verschlüsselns für die übergebenen Daten, Adressaten einschließlich der Prüfung der Gültigkeit ihrer Zertifikate und der Zulässigkeit der Verschlüsselungsrichtlinie.
- O.AK.Dec fordert die Bereitstellung des Entschlüsselns für die übergebenen Daten, wenn die Verschlüsselungsrichtlinie und der Sicherheitszustand der Chipkarten mit den benötigten Entschlüsselungsschlüsseln dies erlauben.
- OE.AK.PKI gewährleistet die Bereitstellung der PKI für die Verschlüsselung sowie die Identifizierung und Implementation zulässiger Verschlüsslungsregeln.

OSP.AK.CardService

Die Sicherheitspolitik OSP.AK.CardService wird durch die geeignete Sicherheitsziele O.AK.Chipkartendienst und O.AK.VAD realisiert. Das Sicherheitsziel OE.AK.PKI stellt die benötigten Zertifikate der qualifizierten elektronischen Signatur mit dem HBA, Zertifikate für andere Signaturen, Verschlüsselungszertifikate und CV-Zertifikate für die Kartenhalter und die verwendeten Chipkarten bereit.

OSP.AK.Fachanwendungen

Die Sicherheitspolitik OSP.AK.Fachanwendungen fordert die Vertrauenswürdigkeit der Fachanwendungen, zentralen Dienste der TI-Plattform und deren Intermediäre sowie deren gesicherte Kommunikation. Diese setzen sich aus einem Anteil innerhalb des EVG und einen Anteil in der Einsatzumgebung des EVG zusammen. Der Anteil innerhalb des EVG entspricht den Fachmodulen. Da nur ein Fachmodul im Einsatz ist (VSDM), wird dies durch das entsprechende Sicherheitsziel O.AK.VSDM umgesetzt. Das Sicherheitsziel O.AK.VZD verlangt, die Abfrage des VZD durch Clientsysteme und Fachmodule durch Nutzung des LDAP-Proxies Daten aus dem VZD über gesicherte Kanäle zu unterstützen. Die Anforderungen an die anderen Anteile der Fachanwendung werden durch das Umgebungsziel OE.AK.Fachdienste geeignet umgesetzt.

OSP.AK.VAUSGD

Die Sicherheitspolitik fordert die vor Abhören geschützte Verbindung des TOE in die VAU-Instanz der ePA-Dokumentenverwaltung sowie in das SGD-HSM des Schlüsselgenirierungsdienstes durch die korrekte Implementierung des „VAU-Protokolls“ und des „SGD-Protokolls“. Die OSP wird durch das Sicherheitsziel O.AK.VAUSGD umgesetzt, welches die spezifikationskonforme Implementierung der Protokolle fordert. Die Anforderungen an die korrekte Nutzung der Kommunikationskanäle durch die ePA-Fachanwendungen werden durch das Umgebungsziel OE.AK.Fachdienste geeignet umgesetzt.

4.5.4.3. Annahmen

- Die Annahme A.AK.Cardterminal_eHealth wird durch das Umgebungsziel OE.AK.Kartenterminal geeignet umgesetzt.
- Die Annahme A.AK.Konnektor wird durch das Umgebungsziel OE.AK.Plattform geeignet umgesetzt.
- Die Annahme A.AK.Versicherter wird offensichtlich durch das Umgebungsziel OE.AK.Versicherter abgebildet.
- Die Annahme A.AK.HBA-Inhaber wird offensichtlich durch das Umgebungsziel OE.AK.HBA-Inhaber abgebildet.
- Die Annahme A.AK.SMC-B-PIN wird offensichtlich durch das Umgebungsziel OE.AK.SMC-B-PIN abgebildet.
- Die Annahme A.AK.sichere_TI wird offensichtlich durch das Umgebungsziel OE.AK.sichere_TI abgebildet.
- Die Annahme A.AK.Admin_EVG wird offensichtlich durch das Umgebungsziel OE.AK.Admin_EVG abgebildet.
- Die Annahme A.AK.SMC wird durch das Umgebungsziel OE.AK.SMC geeignet umgesetzt.
- Die Annahme A.AK.QSCD wird durch das Umgebungsziel OE.AK.HBA geeignet umgesetzt.
- Die Annahme A.AK.phys_Schutz wird durch das Umgebungsziel OE.AK.phys_Schutz geeignet umgesetzt.
- Die Annahme A.AK.Chipkarteninhaber wird durch die Umgebungsziele OE.AK.Personal in Bezug auf die Vertrauenswürdigkeit im Umgang mit den ihm anvertrauten zu

schützenden Daten und OE.AK.SecAuthData im Bezug auf den Schutz seiner Authentisierungsdaten geeignet umgesetzt.

- Die Annahme A.AK.Benutzer_Signatur wird durch das Umgebungsziel OE.AK.Benutzer_Signatur geeignet umgesetzt.
- Die Annahme A.AK.gSMC-K wird durch das Umgebungsziel OE.AK.gSMC-K geeignet umgesetzt.
- Die Annahme A.AK.Env_Arbeitsplatz wird durch die Umgebungsziele OE.AK.Clientsystem und OE.AK.ClientsystemKorrekt umgesetzt.

5. Definition zusätzlicher Komponenten

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

Die Definition der Familie FPT_EMS wurde aus dem BSI-CC-PP-0098, [16], übernommen.

Family **FPT_EMS – EVG Emanation**

Family behaviour This family defines requirements to mitigate intelligible emanations.

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

FPT_EMS.1 – EVG Emanation has two constituents:

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

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

Management: FPT_EMS.1
There are no management activities foreseen.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

5.2. Definition der Familie FIA_API Authentication proof of Identity

Die Definition der Familie FIA_API wurde aus dem PP BSI-CC-PP-0098, [16], übernommen.

Family **FIA_API – Authentication proof of Identity**

Family behaviour: This family defines functions provided by the TOE to prove their identity and to be authenticated by an external entity in the TOE IT environment.

Component levelling:

FIA_API – Authentication proof of Identity	1

FPT_ API.1 – Authentication proof of Identity has one constituent:

FIA_API.1.1 „Authentication proof of Identity“ describes the functional requirements for the proof of the claimed identity for the authentication verification with an assigned authentication mechanism.

The verification of the TSF provided authentication proof of the identity or role is performed by the external entity.

Management: There are no management activities foreseen

Audit: There are no actions defined to be auditable, if FAU_GEN is part of the PP/ST.

FIA_API.1 **Authentication proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *identity or role*].

6. Sicherheitsanforderungen

6.1.1. Hinweise zur Notation

Die Auswahl der funktionalen Sicherheitsanforderungen ist durch das zugrundeliegende Schutzprofil, BSI-CC-PP-0098, gegeben. Das Schutzprofil basiert auf Version 3.1 Revision 5 der Common Criteria; diese Version [5] liegt in englischer Sprache vor. Operationen wurden dabei teilweise in deutscher Sprache ausgeführt.

Dieses Security Target übernimmt die Formulierungen des Schutzprofils PP [16].

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

Die Operation **Verfeinerung** (refinement) wird genutzt, um Details zu einer Anforderung hinzuzufügen und schränkt diese Anforderung folglich weiter ein. In diesem Security Target werden Verfeinerung durch **fettgedruckten Text** in der Anforderung hervorgehoben und in einem der Anforderung folgenden Anwendungshinweis näher erläutert. Gelöschter Text wird ~~**fettgedruckt und durchgestrichen**~~ dargestellt.

Die Operation **Auswahl** (selection) wird genutzt, um eine oder mehrere durch die CC vorgegebenen Optionen auszuwählen. In diesem Security Target wird eine bereits im PP [16] ausgeführte Auswahl durch unterstrichenen Text in der Anforderung hervorgehoben. Eine durch das PP bzw. durch die CC vorgegebene und im Security Target ausgeführte Auswahl wird zusätzlich durch [eckige Klammern] hervorgehoben. Für die Operationen ist durch eine Fußnote jeweils der Originaltext bzw. der Text des PP [16] angegeben.

Die Operation **Zuweisung** (assignement) wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Security Target werden bereits im PP [16] ausgeführte Zuweisungen durch *kursiven Text* in der Anforderung hervorgehoben. Durch das PP bzw. durch die CC vorgegebene und im Security Target ausgeführte Zuweisungen werden zusätzlich durch [*eckige Klammern*] hervorgehoben. Für die Operationen ist durch eine Fußnote jeweils der Originaltext bzw. der Text des PP [16] angegeben.

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

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Diese Sicherheitsvorgaben betrachten für jeden in Tabelle 8 definierten Benutzer gesonderte Subjekte, die in deren Auftrag handeln, d.h. für jeden Benutzer des Clientsystems auf den Arbeitsplätzen (des Clientsystems), den Anwendungskonnektor, jedes eHealth-Kartenterminal, und für jede gesteckte Chipkarte in jedem Chipkartensteckplatz eines jeden mit dem Konnektor verbundenen eHealth-Kartenterminal werden gesonderte Subjekte betrachtet. Zur Unterscheidung zwischen diesen Subjekten und den externen Benutzern werden die Subjekte in Parenthese gesetzt, z. B. bezeichnet HBA den Heilberufsausweis in der Einsatzumgebung

und S_HBA das Subjekt, welches den Heilberufsausweis als Datenquelle und Datensenke mit seinem Sicherheitsstatus EVG-intern abbildet.

Für interne Prozesse, die von den Benutzern angefordert, aber unter interner Steuerung ablaufen, werden die gesonderten Subjekte Signaturdienst, Verschlüsselungsdienst, Chipkartendienst und Kartenterminaldienst definiert. Die Sicherheitsattribute der Benutzer bzw. Subjekte sind in Tabelle 8 definiert.

6.1.2.1. Subjekte

Subjekt	Beschreibung	Sicherheitsattribut
S_Administrator	Subjekt, das für einen Administrator handelt.	Siehe Tabelle 8.
S_Signaturdienst	Dienst des EVG zur Erstellung und Prüfung qualifizierter und nichtqualifizierter elektronischer Signaturen	Das Subjekt übernimmt die Sicherheitsattribute des aufrufenden Benutzers
S_Verschlüsselungsdienst	Dienst des EVG zur Verschlüsselung und Entschlüsselung von Dokumenten	Kein Sicherheitsattribut
S_Chipkarten-dienst	Dienst des EVG zur Verwaltung und zum Zugriff auf gesteckte Chipkarten	Kein Sicherheitsattribut
S_Kartenterminaldienst	Dienst des EVG zur Verwaltung und zum Zugriff auf eHealth-Kartenterminals	Kein Sicherheitsattribut
S_TSL_Dienst	Zentraler TSL-Dienst der TI nach [40]. Stellt die TSL und die BNetzA-VL sowie deren Hash zum Download in der TI bereit. Für den Download BNetzA-VL und deren Hash wird der TSL-Dienst über das TLS-Protokoll angesprochen.	Kein Sicherheitsattribut
S_KSR	„Update-Server“ in der TI. Stellt freigegebene Firmware-Update-Pakete für den TOE und eHealth Kartenterminals zum Download bereit.	Kein Sicherheitsattribut

Subjekt	Beschreibung	Sicherheitsattribut
S_AK	Subjekt, das für einen Prozess des AK handelt, der für einen Funktionsaufruf des Clientsystems oder eines Fachmoduls handelt.	**Aufrufender**: Das Sicherheits-attribut gibt an, ob der Aufruf durch ein Clientsystem oder ein Fachmodul erfolgte.
S_NK	Subjekt, das für einen Prozess des NK handelt.	Kein Sicherheitsattribut
S_Benutzer_Clientsystem	Subjekt, das für den Benutzer des Clientsystems handelt. Der Benutzer wird durch den EVG identifiziert, und die korrekte Authentisierung gegenüber der zu benutzenden Chipkarte autorisiert. Im Fall der Stapelsignatur für die qualifizierte elektronische Signatur muss eine Autorisierung des Benutzers für das Signieren eines jeden einzelnen Dokuments bei Einfachsignatur oder eines Stapels bei der Stapelsignatur erfolgen. Im Fall der Komfortsignatur muss die Autorisierung einmalig bei Aktivierung der Komfortsignatur für eine HBA-Kartensitzung erfolgen.	**Identität des Benutzers**: Datum zur Identifizierung des Benutzers des Clientsystems. Diese Identität muss den Chipkarten HBA, SMC-B und ggf. eGK zugeordnet werden können. **Authorisierungsstatus**: Status der Zuordnung des Benutzers des Clientsystems zu dem Authentisierungsstatus der Chipkarte in Abhängigkeit von der gewünschten Funktion. Werte: - „nicht autorisiert“: Zuordnung nicht durch Chipkarte bestätigt, - „autorisiert“: Zuordnung durch Chipkarte bestätigt.
S_eHKT	Subjekt des eHealth-Kartenterminals, das mit dem eHealth-Kartenterminal kommuniziert. eHealth-Kartenterminals besitzen mindestens 1 ID-000 Kartensteckplatz und mindestens 1 ID-1 Kartensteckplatz zur Aufnahme von Chipkarten.	**Identität**: Umfasst die - ID.SMKT.AUT des eHealth-Kartenterminals, - physische Adresse im LAN-LE. **Arbeitsplatz**: zugeordneter Arbeitsplatz des eHealth-Kartenterminals. **Kartenslot**: Adresse des Kartenslots und die darin gesteckte Chipkarte. **Authentisierungsstatus**: - „nicht identifiziert“ – Kartenterminal unbekannter

Subjekt	Beschreibung	Sicherheitsattribut
		Identität ohne vereinbarte Pairing-Geheimnis - „identifiziert“ – Identität des eHealth-Kartenterminals ist bekannt, Pairing-Geheimnis bekannt, - „authentisiert“ – erfolgreiche Authentisierung mit der SMC als gSMC-KT und mit Pairing-Geheimnis, bestehender TLS-Kanal
S_HBA	Subjekt, das einem HBA in einem Chipkartensteckplatz eines eHealth-Kartenterminals zugeordnet ist	**Identität**: - ICCSN, - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten - eindeutige Referenz des Entschlüsselungsschlüssel-inhabers für verschlüsselte Daten.[26] **Kartenhandle**: identifiziert den HBA in einem Chipkartensteckplatzeines eHealth-Kartenterminals.
S_gSMC-KT	Subjekt, das einer Chipkarte gSMC-KT in einem Chipkartensteckplatz eines eHealth-Kartenterminals zugeordnet ist.	**Identität**: ICCSN **Kartenhandle**: identifiziert die gSMC-KT in einem Chipkartensteckplatzeines eHealth-Kartenterminals.
S_SMC-B	Subjekt, das einer Chipkarte SMC-B in einem Chipkartensteckplatz eines eHealth-Kartenterminals zugeordnet ist..	**Identität**: - ICCSN,

[26] Durch organisatorische Maßnahmen ist sicherzustellen, dass die Identität des Benutzers des Clientsystems (S_Benutzer_Clientsystem) und die Identität des Signaturschlüssel-Inhabers der zu signierenden Daten sowie des vorgesehenen Empfängers zu entschlüsselnder Daten eindeutig einander zugeordnet werden können.

Subjekt	Beschreibung	Sicherheitsattribut
		- eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten - eindeutige Referenz des Entschlüsselungsschlüssel-inhabers für verschlüsselte Daten.[27] **Kartenhandle**: identifiziert die SMC-B in einem Chipkartensteckplatzeines eHealth-Kartenterminals. **Mandant**: Zuordnung zu einem Mandanten.
S_eGK	Subjekt, das einer Chipkarte eGK in einem Chipkartensteckplatz eines eHealth-Kartenterminals zugeordnet ist.	**Identität**: - ICCSN, - Identität des Chipkarteninhabers. **Kartenhandle**: identifiziert die eGK in einem Chipkartensteckplatzeines eHealth-Kartenterminals.
S_Clientsystem	Ein Clientsystem, das zum AK einen TLS-Kanal aufbauen kann und das den AK an dessen LAN Schnittstelle aufruft	**Schlüsselmaterial:** Authentifizierungsmerkmal, mit dessen Hilfe der AK die Authentizität des Clientsystems überprüfen kann **Mandant**: Zuordnung zu einem Mandanten
S_Fachmodul	Subjekt, das für ein installiertes Fachmodul agiert. Fachmodule sind Teile von Fachanwendungen die auf dem Konnektor ablaufen (siehe auch Fachmodul im Glossar).	**Identität:** eindeutiger Name zur Identifizierung des Fachmoduls

[27] Durch organisatorische Maßnahmen ist sicherzustellen, dass die Identität des Benutzers des Clientsystems (S_Benutzer_Clientsystem) und die Identität des Signaturschlüssel-Inhabers der zu signierenden Daten sowie des vorgesehenen Empfängers zu entschlüsselnder Daten eindeutig einander zugeordnet werden können.

Subjekt	Beschreibung	Sicherheitsattribut
S_VSDM_Fachmodul	Subjekt des VSDM Fachmodules	**Identität:** eindeutiger Name zur Identifizierung des Fachmoduls
S_VSDM_Intermediär	Subjekt, das für den dem Fachdienst VSDD zugeordnete Intermediär agiert, zu dem der AK einen TLS Kanal aufbauen kann	**Schlüsselmaterial:** Authentifizierungsmerkmal, mit dessen Hilfe der AK die Authentizität des Intermediär überprüfen kann
S_ Fachdienst	Subjekt, das für einen Fachdienst agiert. Fachdienste sind Teile von Fachanwendungen, die entfernt ablaufen (siehe auch Fachdienst im Glossar).	**Identität:** eindeutiger Name zur Identifizierung des Fachdienstes
S_VSDD_Fachdienst	Subjekt, das für den Fachdienst VSDD agiert, zu dem der AK einen logischen Kanal mit der eGK vermittelt.	**Schlüsselmaterial:** Authentifizierungsmerkmal, mit dessen Hilfe die eGK die Authentizität des VSDD überprüfen kann
S_CMS	Subjekt, das für den Card Management Service Dienst agiert, zu dem der AK einen logischen Kanal mit der eGK vermittelt.	**Schlüsselmaterial:** Authentifizierungsmerkmal, mit dessen Hilfe die eGK die Authentizität des CMS überprüfen kann
PIN-Terminal	Das PIN_Terminal dient zur Eingabe der PIN im Rahmen der Operationen zur entfernten oder lokalen PIN-Eingabe. Als PIN-Terminal werden eHealth-Kartenterminals genutzt, siehe auch S_eHKT.	Siehe S_eHKT
S_HBAx	Subjektbezeichner, welcher sowohl den HBA, als auch die HBA-Vorläuferkarten (HBA-VK) adressiert (siehe auch HBAx im Glossar) .	**Identität:** Sicherheitsattribut „HBA“ bzw. „HBA-VK“.

Subjekt	Beschreibung	Sicherheitsattribut
S_Verzeichnisdienst (VZD)	Zentraler Verzeichnisdienst (VZD) in der TI nach [41]. Der VZD Enthält Einträge von Leistungserbringern und Institutionen mit allen definierten Attributen.	Kein Sicherheitsattribut
S_Benutzern	Menge der folgenden Subjekte: a) S_AK b) S_Signaturdienst c) S_Benutzer_Clientsystem	Siehe entsprechende Attribute der einzelnen Sublekte.

Tabelle 14: Subjekte

6.1.2.2. Objekte

Diese Sicherheitsvorgaben betrachten für die definierten Werte gesonderte Objekte und deren Sicherheitsattribute. Die definiert zusätzliche Objekte als Ressource, die der Zugriffskontrolle unterliegen und keine Datenobjekte sind, sowie deren Sicherheitsattribute.

Objekt	Beschreibung	Sicherheitsattribut
Chipkarte	KVK, eGK, HBA, gSMC-K, SMC-B oder gSMC-KT	**Identität**: ICCSN **Kartentyp**: KVK, eGK, HBA, gSMC-K, SMC-B oder gSMC-KT mit den dafür zulässigen Rollen **Kartenhandle:** identifziert eine in einem eHealth-Kartenterminal gesteckte Chipkarte **Identität des Kartenslots**: Kartenslot des eHealth-Kartenterminals, in dem die Chipkarte gesteckt ist. **Identität des eHealth-Kartenterminal**: eHealth-Kartenterminal, an dem die Chipkarte gesteckt ist.

Objekt	Beschreibung	Sicherheitsattribut
Logischer Kanal einer Chipkarte	Logischer Kanal eines HBA, einer SMC oder einer eGK.	**Sicherheitszustand**: Sicherheitszustand des logischen Kanals der Chipkarte (vergl. COS-Spezifikation [31]).
SICCT-Kommando	Kommandos zur Steuerung der eHealth-Kartenterminals. Die SICCT-Kommandos dienen [38] [42] - der Steuerung des eHealth-Kartenterminals, insbesondere zur Kommunikation mit dem Konnektor, Kommandoabarbeitung und Konfiguration der eHealth-Kartenterminals (hier kurz „eHKT-Steuerungskommando“ genannt), - dem Zugriff auf die Anzeige (Display und Anzeige des gesicherten PIN-Modus), und die Tastatur (lesend) sowie ggf. dem Tongeber (hier kurz „Benutzer-kommuikationskommando“ genannt), - der Kontrolle, Aktivierung, Deaktivierung und Statusabfrage des elektrischen Zustands von Chipkartenkontaktiereinheiten und der Kommunikation mit Chipkarten in den Chipkartenslots (hier kurz „Chipkartenkommando“ genannt), und - die Auslösung der Prozesse zur PIN-Eingabe und dem PIN-Wechsel im gesicherten Modus (hier kurz „PIN-Prozesskommando“ genannt).	**Typ des SICCT-Kommandos**: - eHKT-Steuerungskommando, - Benutzerkommuikationskom-mando, - Chipkartenkommando, - PIN-Prozesskommando.
Antwort auf SICCT-Kommando	Antwortnachricht des eHealth-Kartenterminals auf ein zuvor gesendetes SICCT-Kommando, siehe [42].	Kein Sicherheitsattribut

Objekt	Beschreibung	Sicherheitsattribut
Arbeitsplatz	Arbeitsplatz des Benutzers mit Kartenterminal.	**Identität des Arbeitsplatzes**: Name des Arbeitsplatzes. **Identität eHealth-Kartenterminals**: Identität (Adresse) der am Arbeitsplatz verfügbaren eHealth-Kartenterminals.
Zu signierende Dokumente	Daten, deren Authentizität durch die qualifizierte elektronische Signatur oder nichtqualifizierte, elektronische Signaturen geschützt werden sollen und die an den EVG übergeben werden und deren Repräsentation (Hashwert) an die Signaturkarte zum signieren übertragen werden. Die Vertraulichkeit und Integrität zu signierender Dokumente ist zu schützen[28].	**Autorisierungsstatus:** Status der Auswahl der Daten zur Erstellung einer qualifizierten elektronischen Signatur: - „nicht autorisiert“: Auswahl nicht durch Signaturschlüssel-Inhaber bestätigt - „autorisiert“: Auswahl durch Signaturschlüssel-Inhaber bestätigt. **Signaturrichtlinie:** Beschreibung der Regeln, welche Signatur (qualifiziert, nichtqualifizierte) zu erstellen ist, die signierten Dokumente zu formatieren und – im Fall der QES – wie die Daten darzustellen sind.
Signaturstapel	Ein Stapel zu signierender Daten, der (nach erfolgreicher Authentisierung des Signaturschlüsselinhabers mit der Signatur-PIN gegenüber der Signaturchipkarte) durch den Signaturdienst an die Signaturkarte zum Signieren gesendet wird.	Kein Sicherheitsattribut
Signierte Dokumente	Daten, denen eine digitale Signatur zugeordnet ist. Die Vertraulichkeit	**Signaturrichtlinie:** Beschreibung der Regeln, wie die Daten zu prüfen sind.

[28] Der EVG schützt die Vertraulichkeit zu signierender Dokumente, da diese im allgemeinen Fall medizinische Daten sein können und keine explizite Aussage über einen ausschließlichen Schutz der Integrität getroffen werden kann.

Objekt	Beschreibung	Sicherheitsattribut
	signierter Daten ist zu schützen[29]. Die signierten Daten dürfen durch den EVG nicht verändert werden.	**Angegebener Zeitpunkt:** angenommener Zeitpunkt der Signturerzeugung auf den sich die Prüfung der qualifizierten elektronischen Signatur bezieht. **Ordnungsgemäßigkeit der Signatur:** Daten besitzen eine „ordnungsgemäße“ Signatur, wenn die Signaturen zu Daten eines Stapels zu signierender Daten gehören, mit dem Signaturschlüssel des Heilberufsausweises des autorisierten Benutzers des Clientsystems (S_Benutzer_Clientsystem) erzeugt wurden und wenn zum dazu gehörigen Signaturprüfschlüssel zum Signaturzeitpunkt (unter Beachtung der Grace Period) ein gültiges qualifiziertes Zertifikat existiert. Eine Signatur ist „ungültig“, wenn sie zu anderen Daten ausserhalb des Stapels zu signierender Daten gehören oder nicht mit dem öffentlichen Schlüssel des gültigen qualifizierten Zertifikats des autorisierten Benutzers des Clientsystems (S_Benutzer_Clientsystem) erfolgreich geprüft werden konnten.
Signaturprüfungs-ergebnis	Ergebnis der Prüfung einer Signatur als qualifizierte elektronische Signatur oder nichtqualifizierte elektronische Signatur, das durch den EVG für vorgelegte signierte Daten und einen angegebenen Zeitpunkt erzeugt und dem Benutzer des Clientsystems über die Schnittstellen bereitgestellt wird.	Kein Sicherheitsattribut

[29] Der EVG schützt die Vertraulichkeit signierten Dokumente, da diese im allgemeinen Fall medizinische Daten sein können und keine explizite Aussage über einen ausschließlichen Schutz der Integrität getroffen werden kann.

Objekt	Beschreibung	Sicherheitsattribut
	Die Vertraulichkeit und Integrität des Prüfergebnisses ist zu schützen[30].	
Zu signierender Bitstring	Bitstring von maximal 512 Bit die dem EVG zur Weitergabe and Chipkarten und Erzeugung digitaler Signaturen zum Zweck der Authentisierung von Benutzern gegenüber anderen Instanzen übergeben werden.	Kein Sicherheitsattribut
Signierter Bitstring	Von den Chipkarten empfangene digitale Signaturen von Bitstrings, die als zu signierende Bitstrings dem EVG übergeben wurden.	Kein Sicherheitsattribut
Zu verschlüsselnde Daten	Klardaten, die für identifizierte Empfänger verschlüsselt werden sollen. Die Klardaten und die Empfänger werden vom Aufrufenden dem EVG übergeben und die verschlüsselten Daten an den Aufrufenden zurückgegeben. Die Vertraulichkeit dieser Klardaten ist zu gewährleisten.	**Objekt-ID:** eindeutige Identität der zu verschlüsselnden Daten. **Vorgeschlagene Empfänger:** Identität der Empfänger der zu verschlüsselnden Daten, die vom Aufrufenden (auch zum Auffinden der zugehörigen Verschlüsselungs-zertifikate) vorgeschlagen werden **Verschlüsselungsrichtlinie:** siehe Beschreibung zur Verschlüsselungsrichtlinie im Glossar
Verschlüsselte Daten	Verschlüsselte Daten, die für einen Benutzer entschlüsselt werden sollen. Die verschlüsselten Daten werden vom Aufrufenden dem EVG übergeben und die entschlüsselten Daten an den Aufrufenden zurückgegeben.	**Vorgeschlagene Empfänger:** Identität der Empfänger der zu entschlüsselnden Daten, die vom Aufrufenden (auch zum Auffinden der zugehörigen Entschlüsselungsschlüssel) vorgeschlagen werden. **Verschlüsselungsrichtlinie:** siehe Beschreibung zur

[30] Der Schutz der Vertraulichkeit der Prüfungsergebnisse ergibt sich hier aus dem Bezug zu den vertraulichen zu signierenden bzw. signierten Daten.

Objekt	Beschreibung	Sicherheitsattribut
		Verschlüsselungsrichtlinie im Glossar. **Ordnungsgemäss verschlüsselt:** Status nach erfolgreicher Verschlüsselung wenn (a) die identifizierte Verschlüsselungsrichtlinie gültig ist, (b) zu den vorgesehenen Empfängern gültige Verschlüsselungszertifikate existieren und für die Verschlüsselung des symmetrischen Schlüssels verwendet wurden, (c) die durch den Xpath-Ausdruck selektierten zu verschlüsselnden Daten vollständig verschlüsselt wurden und keine Fehler auftraten.
Zu entschlüsselnde Daten	Verschlüsselte Daten, die für einen Benutzer entschlüsselt werden sollen. Die entschlüsselten Klardaten werden an den Vorgeschlagenen ausgegeben. Die Vertraulichkeit der entschlüsselten Klardaten einschließlich der kryptographischen Schlüssel ist innerhalb der Kontrolle des EVG zu gewährleisten.	**Vorgeschlagene Empfänger:** Identität der Empfänger, für den die Daten entschlüsselt werden, und an den die Daten übergeben werden sollen. **Verschlüsselungsrichtlinie:** siehe Beschreibung zur Verschlüsselungsrichtlinie im Glossar.
Entschlüsselte Daten	Entschlüsselte Daten, die für einen Benutzer entschlüsselt wurden. Die entschlüsselten Klardaten werden an den Aufrufenden zurückgegeben. Die Vertraulichkeit der entschlüsselten Klardaten einschließlich der kryptographischen Schlüssel ist	Kein Sicherheitsattribut

Objekt	Beschreibung	Sicherheitsattribut
	innerhalb der Kontrolle des EVG zu gewährleisten.	
Daten der Chipkarten (Versichertenstammdaten)	Daten der eGK (geschützte Versichertenstammdaten), die durch den Konnektor von den Karten gelesen oder auf die Karte geschrieben werden.	**Versichertenstammdaten (VSD) der eGK:** - geschützt Geschützte Versichertendaten (EF.GVD), die nur nach erfolgreicher Authentisierung ausgelesen werden können. - ungeschützt Teil der VSD bestehend aus persönlichen Daten (EF.PD) und Versichertendaten (EF.VD) die frei auslesbar sind.
Objektsystem der Chipkarte (eGK)	Objektsystem der eGK nach [32],	Kein Sicherheitsattribut
Konnektor/eHKT-Kommunikation	Kommunikation zwischen dem Konnektor und den eHKT in Form von SICCT-Kommandos des Konnektors an die eHKT und Antworten der eHKT und den Konnektor[31]	Kein Sicherheitsattribut
Authentisierungs-verifikationsdaten (VAD)	Datum, das vom Benutzer zum Nachweis seiner Identität gegenüber Chipkarten dient. Dies sind VAD der Kartenhalter und die SVAD[32] als Signaturschlüssel-Inhaber gegenüber der qualifizierten Signaturerstellungseinheit. Die VAD werden zur Authentisierung des Benutzers und zum Wechsel der VAD durch den Benutzer unter Steuerung des EVG an dem PIN-	Kein Sicherheitsattribut

[31] Die “Konnektor/eHKT-Kommunikation” schließt alle “Daten der Chipkarten“ ein, geht aber darüber hinaus, z. B. wird der sichere PIN-Modus durch die SICCT-Kommandos gesteuert sendet die eingegebene PIN direkt an eine gesteckte Chipkarte und nur der Returncode der Chipkarte wird an den Konnektor zurückgegeben.

[32] Englisch: signatory verification authentication data.

Objekt	Beschreibung	Sicherheitsattribut
	Terminal eingegeben und an die Chipkarte übergeben. Dieses Datum kann eine PIN oder eine PUK sein[33]. Die Vertraulichkeit und Integrität[34] der VAD müssen geschützt werden.	
Authentisierungs-referenzdaten der Identität „SAK“	Kartenprüfbares Zertifikat C.SAK.AUTD_CVC, welches von dem EVG zum Nachweis seiner Identität gegenüber dem HBA und der SMC präsentiert wird und den öffentlichen Schlüssel PuK.SAK.AUTD_CVC enthält, der zum privaten Schlüssel PrK.SAK.AUTD_CVC korrespondiert.	Kein Sicherheitsattribut
Authentisierungs-referenzdaten des AK	Kartenprüfbares Zertifikat C.SAK.AUT, welches von dem AK zum Nachweis seiner Identität gegenüber den eHealth-Kartenterminals[35] präsentiert wird und den öffentlichen Schlüssel PuK.SAK.AUT enthält, der zum privaten Schlüssel PrK.SAK.AUT korrespondiert.	Kein Sicherheitsattribut
Zu sendende Daten	zu schützende Daten, die vom Konnektor an eine andere Komponente der Telematikinfrastruktur übertragen werden. Die zu übertragenden Daten werden vor Übertragung verschlüsselt und integritätsgeschützt	Kein Sicherheitsattribut
Empfangene Daten	zu schützende Daten, die von einer anderen Komponente der Telematikinfrastruktur an den Konnektor übertragen werden. Die	Kein Sicherheitsattribut

[33] Der Heilberufsausweis als qualifizierte Signaturerstellungseinheit unterstützt nur die Authentisierung durch Wissen.

[34] Der Schutz der Integrität ist insbesondere bei einem Wechsel der SVAD erforderlich.

[35] C.SAK.AUT kann nach gSMC-K-Spezifikation auch für die interne Kommunikation benutzt werden. Dies ist keine Verwendung als Authentisierungsreferenzdatum für externe Benutzer.

Objekt	Beschreibung	Sicherheitsattribut
	empfangenen Daten werden entschlüsselt und integritätsgeprüft. Es werden unverfälscht empfangene Daten ausgegeben.	
Datenobjekte des sicheren Datenspeichers (Datenobjekt des SDS)	Datenobjekte, die im sicheren Datenspeicher gespeichert sind.	**Administrator**: Werte „Administratorobjekt“ und „allgemeines Datenobjekt“
Schlüssel für sicheren Datenspeicher	Der Zugriff auf den Inhalt des sicheren (geschützten) Datenspeichers durch den Konnektor ist durch Nutzung von Schlüsselmaterial abgesichert. Datenobjekte im sicheren Datenspeicher dürfen nur verschlüsselt gespeichert werden.	Kein Sicherheitsattribut
eHealth-Kartenterminal	Ein im LAN des Leistungserbringers vorhandenes und gepaartes eHealth-KT	**Arbeitsplatz**: zugeordneter Arbeitsplatz des eHealth-Kartenterminals: • eindeutige Identifikation • erlaubte Zuordnungen als lokales KT zu einem Arbeitsplatz • erlaubte Zuordnungen als entferntes KT zu einem Arbeitsplatz • erlaubte Zuordnungen als entferntes PIN-Eingabe-KT für eine Kombination aus Mandant und Arbeitsplatz • erlaubte Zuordnungen zu einem Mandanten
Kartensitzung eGK	Kartensitzung einer eGK	Für jede eGK-Kartensitzung: • Bindung an den Arbeitsplatz, von dem aus

Objekt	Beschreibung	Sicherheitsattribut
		zuerst auf die eGK zugegriffen wurde • Karte, welche die eGK im Rahmen einer Card-to-Card- Authentisierung freigeschaltet hat
Kartensitzung HBA	Kartensitzung einer HBA	Für jede HBA-Kartensitzung: • Bindung an das Primärsystem und die UserID, unter deren Kontext zuerst auf den HBA zugegriffen wurde
Kartensitzung SMC-B bzw. SM-B	Kartensitzung einer SMC-B bzw. SM-B-Sitzung	Für jede SMC-B- bzw. SM-B-Sitzung: • Bindung an den Mandanten, von dem aus auf die SMC-B bzw. SM-B zugegriffen wurde • Karte, welche die SMC-B bzw. SM-B im Rahmen einer Card-to-Card-Authentisierung freigeschaltet hat
Clientsystem	Ein im LAN des Leistungserbringers vorhandenes Clientsystem	**Für jedes Clientsystem:** • eindeutige Identifikation, • Authentisierungsmerkmal (z. B. TLS-Zertifikat), • erlaubte Zuordnungen zu Arbeitsplätzen • erlaubte Zuordnungen zu Mandanten Neben diesen statischen Sicherheitsattributen verwaltet der AK für das Clientsystem das folgende **dynamische Sicherheitsattribut**: • dynamische exklusive Bindung einer HBA-Kartensitzung an ein Clientsystem

Objekt	Beschreibung	Sicherheitsattribut
Mandant	Nach dem Informationsmodell werden Mandanten dem Clientsystem sowie vom Konnektor verwalteten externen Ressourcen (Kartentermi-nal mit Slots, Arbeitsplatz mit Signaturproxy und SMC-Bs) persistent zugeordenet .	Kein Sicherheitsattribut
verwaltete SMC-B	Ein im LAN des Leistungserbringers verwaltetes SMC-B, siehe Infomodell in Spezifikation Konnektor	Für jede verwaltete SMC-B • eindeutige Identifikation • der SMC-B fest zugeordnete Mandanten
TLS-Kanal	Transport Layer Security. Protokoll zur Verschlüsselung von Datenübertragungen, das einen sicheren Kanal zwischen Anwendungskonnektor und Fachdiensten oder Zentralen Diensten der TI bietet.	Anfordernder TLS-Client: Identität des Clientsystems (Fachmodul), das den Aufbau des TLS-Kanals angefordert hat. Der Anwendungskonnektor S_AK steuert und verwaltet den TLS-Kanal zum Fachdienst für das Fachmodul.
Eingeschränkter Text	Text, der keine unerlaubten Zeichenketten enthält, die den Benutzer des Kartenterminals zur Eingabe einer PIN oder PUK im ungeschützten Mode verleiten könnte. Beispiele für unerlaubte Zeichenketten sind „PIN“, PUK“, „Geheimzahl“ oder „Code“ und deren Abwandlungen durch Groß-Kleinschreibungen oder andere irreführende Schreibweisen (vergl. [27], Kap. 4.1.4.4)	Kein Sicherheitsattribut
Update-Pakete	Software-Komponenten eines zukünftigen EVG, die im Sinne eines Update Prozesses zur Aktualisierung der laufenden Version der Software-Komponente des EVG dienen soll	**Signatur**: Intergritätsschutz des Update-Paketes **Zulässige Software-Versionen:** Firmware-Gruppe nach [69]. In jeder Konnektor-Software muss

Objekt	Beschreibung	Sicherheitsattribut
		eine versionierte Liste zulässiger Firmware-Versionen für Software-Updates integriert sein.
Signaturschlüssel externer Signaturchipkarten	Schlüssel des HBA oder der SM-B der vom Signaturdienst des Anwendungskonnektors für die erstellung von Signaturen verwedet wird.	Kein Sicherheitsattribut
Authentisierungsschlüssel von HBAx oder SM-B	Schlüssel des HBAx oder der SM-B der für die Authentsierung zum Signaturdienst verwendet wird.	Kein Sicherheitsattribut

Tabelle 15: zusätzliche Objekte

Die Operationen der Subjekte auf Objekte sind in den Tabellen Tabelle 17, Tabelle 18, Tabelle 19, Tabelle 20, Tabelle 21 und Tabelle 23 nach den jeweiligen Komponenten FDP_ACF definiert.

6.1.2.3. TSF Daten

TSF Datum	Beschreibung
Öffentlicher Schlüssel zur Prüfung der BNetzA-VL BNetzA-VL.	Öffentlicher Schlüssel zur Prüfung der XML-Signatur der BNetzA-VL. Dieser Schlüssel des Signer-Zertifikats, mit dem die Signatur der Vertrauensliste (BNetzA-VL) geprüft wird, stellt den QES-Vertrauensanker dar. Die Integrität dieses Schlüssels ist zu schützen. Das BNetzA-VL-Signer-Zertifikat wird durch die Bundesnetzagentur veröffentlicht. Es ist in der TSL enthalten und wird über diese aktualisiert. Entsprechend wird ein neuer QES-Vertrauensanker beim Aktualisierungsprozess der TSL nur durch die Signatur der TSL geschützt, welche mittels des öffentlichen Schlüssel zur Prüfung von TSL geprüft wird
Öffentlicher Schlüssel zur Prüfung von TSL	Öffentlicher Schlüssel zur Prüfung der XML-Signatur der TSL. Das zur Prüfung des TSL-Signer-Zertifikates notwendige TSL-Signer-CA-Zertifikat ist bei Auslieferung in der gSMC-K vorhanden und kann im Rahmen eines geplanten Wechsels des TI-Vertrauensankers durch ein Folgezertifikat ersetzt werden.
Öffentlicher Schlüssel der Sub-CA der Verschlüsselungs zertifikate (CA certificates of an encryption PKI)	Öffentliche Schlüssel einer Sub-CA, die Zertifikate für die Verschlüsselung von Daten erstellen. Der EVG kann einen oder mehrere dieser öffentlichen Schlüssel speichern. Die Verteilung dieser Schlüssel erfolgt durch die TSL. Die Integrität dieses Schlüssels bzw. dieser Schlüssel ist zu schützen.

TSF Datum	Beschreibung
Öffentlicher Schlüssel der Wurzelinstanz der CVC (public keys of the CVC root CA)	Öffentlicher Schlüssel PuK.RCA.CS der Wurzelinstanz und somit Vertrauensanker der kartenprüfbaren Zertifikate (CVC) des Gesundheitswesens. Der Schlüssel ist fester Bestandteil des EVG und kann nicht geändert werden. Die Integrität dieses Schlüssels bzw. dieser Schlüssel ist zu schützen. Man beachte, dass PuK.RCA.CS auch auf anderen technischen Komponenten, die CVC besitzen, gespeichert sein kann. Diese dürfen aber nicht für die Prüfung dieser (oder anderer) Komponenten verwendet werden. Die CVC-Zertifikate der CA, die ebenfalls auf diesen Komponenten gespeichert sein können, sind nur ein Zwischenschritt in der CVC-Kette und dürfen nicht ungeprüft verwendet werden.
Authentisierungs-verifikationsdaten der Identität „SAK“.	Privater Schlüssel PrK.SAK.AUTD_CVC, welcher von der SAK zum Nachweis ihrer Identität gegenüber dem HBA benutzt wird und zum öffentlichen Schlüssel PuK.SAK.AUTD_CVC im Zertifikat C.SAK.AUTD_CVC korrespondiert.
Authentisierungs-verifikationsdaten der AK	Privater Schlüssel PrK.SAK.AUT, welcher von dem AK zum Nachweis seiner Identität gegenüber den eHealth-Kartenterminals benutzt wird und zum öffentlichen Schlüssel PuK.SAK.AUT im Zertifikat C.SAK.AUT korrespondiert.
Authentisierungs-referenzdaten der eHealth-Karten-terminals	Identität für die Identifizierung und Authentisierungsreferenzdaten (Pairing-Daten) für die Authentisierung jedes mit dem AK gepaarten eHealth-Kartenterminals.
Authentisierungs-referenzdaten des Administrators	Identität für die Identifizierung und Authentisierungsreferenzdaten für die Authentisierung des Administrators.
Identität des Arbeitsplatzes	Identität des Arbeitsplatzes des Benutzers für die Anforderung von Sicherheitsdiensten des EVG, die vom Clientsystem an den EVG übergeben wird.
Arbeitsplatz-konfigurations-daten	Die Zuordnung der Identität des Arbeitsplatzes zu dem am Arbeitsplatz zur Verfügung stehenden eHealth-Kartenterminals mit deren Anzeige, PIN-Pad und den Chipkartenslots. Für die eHealth-Kartenterminals wird nach dem Aufstellungsort und dem Zugriff durch der Benutzer des Arbeitsplatzes unterschieden zwischen (a) den lokal am Arbeitsplatz aufgestellten eHealth-Kartenterminals, deren gesteckte Chipkarten er zugreifen, dessen PIN-Pad er bedienen und dessen Anzeige des Arbeitsplatzes er sehen kann, und (b) den entfernt vom Arbeitsplatz aufgestellten eHealth-Kartenterminals, auf deren gesteckte Chipkarten er remote zugreifen darf, ohne das PIN-Pad bedienen oder die Anzeige sehen zu können.
Kartenhandle	Daten zur Identifizierung einer gesteckten Chipkarte in einem konfigurierten eHealth-Kartenterminal.

Tabelle 16: Übersicht über TSF Daten

6.2. Funktionale Sicherheitsanforderungen des Netzkonnektors

Die funktionalen Sicherheitsanforderungen werden im Folgenden nicht wie sonst häufig in alphabetischer Reihenfolge aufgezählt, sondern nach funktionalen Gruppen gegliedert. Dadurch soll ein besseres Verständnis der Anforderungen und ihrer Abhängigkeiten untereinander erreicht werden. Die funktionalen Gruppen orientieren sich an den in Abschnitt 1.3.5 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

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

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

6.2.1. VPN-Client

VPN

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

Dependencies: No dependencies.

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

Telematikinfrastruktur[36] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[37] and protection of the channel data from modification *and*[38] disclosure.

FTP_ITC.1.2/NK.VPN_TI The TSF shall permit the TSF[39] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_TI The TSF shall initiate communication via the trusted channel for *communication with the TI*[40].

Refinement: Die Anforderung „protection of the channel data from modification and disclosure“ in FTP_ITC.1.1/NK.VPN_TI ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Der Trusted Channel muss auf Basis des **IPsec**-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [27], RFC 4301 (IPsec) [56], RFC 4303 (ESP) [59]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [60]) unterstützt werden.

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

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

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

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

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_SIS The TSF shall provide a communication channel between itself and another trusted IT product **Sicherer Internet Service (SIS)**[41] that is logically distinct from other communication channels

36 refinement

37 refinement

38 refinement (or → and)

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

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

41 refinement

and provides assured identification of its end points **using certificate based authentication**[42] and protection of the channel data from modification **and**[43] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[44] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_SIS The TSF shall initiate communication via the trusted channel for all *communication with the SIS*[45].

Refinement: Die Anforderung „protection of the channel data from modification and disclosure“ in FTP_ITC.1.1/NK.VPN_SIS ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten) aller Kommunikation mit dem Internet. Der Trusted Channel muss auf Basis des **IPsec**-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [27], RFC 4301 (IPsec) [56], RFC 4303 (ESP) [59]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [60]) unterstützt werden.

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

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

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

Anwendungshinweis 77: Der EVG unterstützt RFC 7296 (IKEv2) [60], siehe [30], Kapitel 3.3.1. Dieser Hinweis bezieht sich auf FTP_ITC.1.1/NK.VPN_SIS und FTP_ITC.1.1/NK.VPN_TI.

Anwendungshinweis 78: Die Kommunikation von EVGs untereinander ist nicht vorgesehen.

Informationsflusskontrolle

Die von O.NK.PF_WAN und O.NK.PF_LAN erzwungene VPN-Nutzung für *zu schützende Daten der TI und der Bestandsnetze* und für *zu schützende Nutzerdaten* (im Sinne des Abschnitts 3.1) wird durch FDP_IFF.1.2/NK.PF umgesetzt, sofern die Paketfilter-Regeln

---

42 refinement

43 refinement (or → and)

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

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

geeignet gesetzt sind, was wiederum durch die Administratordokumentation (siehe das Refinement zu AGD_OPE.1 in Abschnitt 6.2.8) sichergestellt wird.

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Dynamischer Paketfilter

FDP_IFC.1/NK.PF Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

hier erfüllt durch: FDP_IFF.1/NK.PF

FDP_IFC.1.1/ NK.PF The TSF shall enforce the *packet filtering SFP (PF SFP)*[46] on *the subjects*

(1) IAG,

(2) VPN concentrator of the TI,

(3) VPN concentrator of the SIS,

(4) the TI services ,

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

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

(7) active entity in the LAN,

(8) CRL download server,

(9) TSL-Dienstserver

(10) hash&URL server,

(11) registration server of the VPN network provider,

(12) remote management server,

the information

(1) incoming information flows

(2) outgoing information flows

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[47].

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

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

Anwendungshinweis 79: Die dynamischen Paketfilter (LAN-seitig und WAN-seitig) sollen sowohl den EVG vor Angriffen bzw. vor unerlaubten Informationsflüssen (i) aus dem LAN und (iii) aus dem WAN schützen als auch die Informationsflüsse zwischen (ii) LAN und WAN bzw. (iv) zwischen WAN und LAN kontrollieren.

Anwendungshinweis 80: Systembedingt bietet IPv4 (Internet Protocol, Version 4) nur eine Identifikation der Informationsflüsse, aber keine Authentisierung. Aus Mangel an besseren Mechanismen müssen dennoch auf dieser Basis die Entscheidungen über die Zulässigkeit von Informationsflüssen getroffen werden.

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

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der WAN-Adapter des Konnektors angeschlossen ist.
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der LAN-Adapter des Konnektors angeschlossen ist.
ANLW_LEKTR_INTRANET_ROUTES	Adressbereich des Intranet-VPN des LE
NET_SIS	VPN-Konzentratoren der SIS
NET_TI_ZENTRAL	Zentrale Dienste der TI
NET_TI_DEZENTRAL	Adressbereich der WAN-Schnittstellen der Konnektoren für die Kommunikation mit der TI oder den Bestandsnetzen
NET_TI_OFFENE_FD	Offene Fachdienste der TI
NET_TI_GESICHERTE_FD	Gesicherte Fachdienste der TI
ANLW_BESTANDSNETZE	die an die TI angeschlossenen Bestandsnetze
ANLW_AKTIVE_BESTANDSNETZE	die an die TI angeschlossenen und vom Administrator freigeschalteten Bestandsnetze
VPN_KONZENTRATOR_TI_IP_ADDRESS	IP-Adresse des VPN-Konzentrators der TI
VPN_KONZENTRATOR_SIS_IP_ADDRESS	IP-Adresse des VPN-Konzentrators des SIS
DNS_SERVERS_BESTANDSNETZE	IP-Adressen von DNS-Servern für die Bestandsnetze (ANLW_BESTANDSNETZE)

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
TSL Diensteserver	IP-Adresse des TSL-Diensteserver Hierzu zählen die Download-Bereiche: CERT_TSL_DOWNLOAD_ADDRESS_INTERNET, CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU CERT_TSL_IP_ADDRESS_INTERNET CERT_TSL_IP_ADDRESS_INTERNET_BU
DNS_ROOT_ANCHOR_URL	IP-Adresse des DNSSEC Vertrauensankers für das Internet
hash&URL-Server	IP-Adresse des hash&URL-Servers
registration server	IP-Adresse des Registrierungsservers
remote management server	IP-Adresse des Remote-Managementservers
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.

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

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

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

FDP_IFF.1/NK.PF Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_MSA.3 Static attribute initialisation

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

FDP_IFF.1.1/NK.PF The TSF shall enforce the *PF SFP*[48] based on the following types of subject and information security attributes:

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

(1) IP address,

(2) port number,

(3) protocol type,

(4) *direction (inbound and outbound IP*[49] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES.[50]

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

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

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

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

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

---

48 [assignment: *information flow control SFP*]

49 IP = Internet Protocol

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

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

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

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

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

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

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

(7) *The TSF shall allow*

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

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

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

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

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

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

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

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

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

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

(9) The TSF shall allow

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

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

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

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

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

b) The rules ANLW_FW_SIS_ADMIN_RULES applies if defined.

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

(13) The TSF shall redirect communication from IAG to active entities in the LAN if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and

ANLW_INTERNET_MODUS=IAG und ANLW_IAG_ADDRESS≠““).[51]

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

(1) The TSF shall enforce SFP rules ANLW_FW_SIS_ADMIN_RULES

(2) *The TSF shall transmit data (except for establishment of VPN connections) to the WAN only if the IPsec VPN tunnel between the TSF and the remote VPN concentrator has been successfully established and is active and working*[52].

FDP_IFF.1.4/NK.PF The TSF shall explicitly authorise an information flow based on the following rules*: Stateful Packet Inspection,* [*no additional rules*][53].

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

(12) [*no additional rules*] [54].

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

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

Der Mechanismus „Logische Trennung“ nach [gemSpec_Kon], TIP1-A_4823 wird vom EVG nicht umgesetzt. Das Attribut

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

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

Anwendungshinweis 81: Durch die Festlegung verbindlicher, nicht administrierbarer Paketfilter-Regeln (vgl. auch das Refinement zu FMT_MSA.1/NK.PF) und bei Wahl eines geeigneten Satzes von Paketfilter-Regeln (siehe dazu das Refinement zu AGD_OPE.1 in Abschnitt 6.2.8) erzwingt FDP_IFF.1.2/NK.PF die VPN-Nutzung für zu schützende Daten der TI und der Bestandsnetze und *zu schützende Nutzerdaten* wie in Abschnitt 3.1 definiert.

Anwendungshinweis 82: Der EVG verwaltet Informationen über eine Historie der Verbindung durch die firewall des Betriebsystemkernels (iptables). Es werden eingehende Verbindungen nur als Antworten auf zuvor ausgegangene Anfragen zugelassen, so dass ein ungefragter Verbindungsaufbau aus dem WAN wirkungsvoll verhindert wird. Siehe auch stateful packet inspection im Glossar.

Anwendungshinweis 83: Die dynamische Paketfilterung soll die Menge der **zulässigen Protokolle** im Rahmen der Kommunikation mit der Telematikinfrastruktur geeignet beschränken. Es sind nur die in der Spezifikation Netzwerk [gemSpec_Net] [29], Tabelle 1 aufgeführten Protokolle zulässig. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.

EVG erzwingt, dass *zu schützende Daten der TI und der Bestandsnetze* und *zu schützende Nutzerdaten* über den VPN-Tunnel in die Telematikinfrastruktur bzw. zum Internet versendet werden; EVG verhindert ungeschützten Zugriff auf das Transportnetz. Darüber hinaus wurden keine weiteren regeln (mittels FDP_IFF.1.3/NK.PF bis FDP_IFF.1.5/NK.PF) ergänzt.

Die von FDP_IFF.1.2/NK.PF geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (siehe unten, FMT_MSA.3/NK.PF) und können vom Administrator verwaltet werden (siehe FMT_MSA.1/NK.PF, vgl. Abschnitt 6.2.6 Administration).

FMT_MSA.3/NK.PF Static attribute initialisation

Restriktive Paketfilter-Regeln

Dependencies: FMT_MSA.1 Management of security attributes

hier erfüllt durch: FMT_MSA.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_MSA.3.1/NK.PF The TSF shall enforce the *PF SFP*[55] to provide restrictive[56] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [*role administrator*][57] to specify alternative initial values to override the default values when an object or information is created.

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

Anwendungshinweis 84: Es gibt nur eine Administrator Rolle welche alternative Default-Werte spezifizieren darf. Dabei wird nicht zwischen lokalem und entfernten Management unterschieden.

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

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

6.2.3. Netzdienste

Zeitsynchronisation

FPT_STM.1/NK Reliable time stamps

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

Dependencies: No dependencies.

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

Refinement: Die Zuverlässigkeit (*reliable*) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [51] erreicht.

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

---

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

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

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

Befindet sich der EVG im Online-Modus, muss er die Zeitsynchronisation mindestens bei Start-up, einmal innerhalb von 24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht [*nicht mehr als 330ms*][58] von der Zeitinformation der darüberliegenden Stratum Ebene ab.

Anwendungshinweis 85: Zum Zeitdienst siehe Konnektor-Spezifikation [27], Abschnitt 4.2.5 Zeitdienst.

Anwendungshinweis 86: Die im Refinement geforderte Zeitsynchronisation entspricht den Anforderungen der aktuellen Version der Konnektor-Spezifikation [27]. Es wurde keine verschärfung des Refinement aus dem NK-PP [17] vorgenommen.

Anwendungshinweis 87: Gemäß Konnektor-Spezifikation [27], Abschnitt 3.3 Betriebszustand, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [27]

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

Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand an der Außenhaut des Konnektors anzeigt, um die benannte Anforderung der Spezifikation umzusetzen, siehe LS14 und PS5 in Kapitel 1.3.3 sowie die Anforderungen an die Konnektor Hardware in Kapitel 1.3.6.

Zertifikatsprüfung

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

Prüfung der Gültigkeit von Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.Zert The TSF shall provide the capability to consistently interpret *information – distributed in the form of a* ***TSL (Trust-Service Status List)*** *and* ***CRL (Certificate Revocation List)*** *information – about the validity of certificates and about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects*[59] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[60] when interpreting the TSF data from another trusted IT product.

---

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

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

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

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

Anwendungshinweis 88: Die interpretation rules in FPT_TDC.1.2/NK.Zert entsprechen den Anforderumgen der aktuellen Version der Konnektor-Spezifikation [27]. Der EVG führt keine explizite Prüfung der Algorithmen auf deren Gültigkeit gegenüber den Vorgaben in TR-03116-1[19] durch. Die Verwendung von gültigen Algorithmen wird durch das Aufbringen eines korrekten und evaluierten Softwarestandes des EVG unter Nutzung des sicheren Updatemechanismus sichergestellt.

Anwendungshinweis 89: Die **TSL** und die **CRL** muss gemäß Anforderung A_4684 in der Konnektor-Spezifikation [27] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden.

Der Konnektor kann die **TSL** bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [27]). Die Liste der entsprechenden Zertifikate aus der TSL wird im Netzkonektor hinterlegt.

6.2.4. Stateful Packet Inspection

Anwendungshinweis 90: Weitergehende Angriffe gegen die Systemintegrität des EVG werden abgewehrt (robuste Implementierung, Resistenz gegen Angriffe wie von AVA_VAN.5 gefordert), aber nicht im Detail erkannt, es gibt keine komplexe Erkennungslogik für Angriffe.

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

6.2.5. Selbstschutz

FDP_RIP.1/NK Subset residual information protection

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

Dependencies: No dependencies.

FDP_RIP.1.1/NK The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[61] the following objects: *cryptographic keys (and session keys) used for the VPN or for TLS-connections, user data (zu schützende*

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

Daten der TI und der Bestandsnetze and zu schützende Nutzerdaten), [*none*][62].

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

Anwendungshinweis 91: Der EVG speichert zu schützende Daten der TI und der Bestandsnetze oder zu schützende Nutzerdaten niemals dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z. B. während einer Ver- oder Entschlüsselung).

Selbsttests

FPT_TST.1/NK TSF testing

Selbsttests

Dependencies: No dependencies.

FPT_TST.1.1/NK The TSF shall run a suite of self tests [during initial start-up][63] to demonstrate the correct operation of [the TSF][64].

FPT_TST.1.2/NK The TSF shall provide authorised users with the capability to verify the integrity of TSF data[65].

FPT_TST.1.3/NK The TSF shall provide authorised users with the capability to verify the integrity of [TSF][66].

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

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

Anwendungshinweis 92: Die kryptographischen Verfahren werden in Software implementiert. Der Benutzer kann die Selftests durch Neustart des EVGs selbst anstoßen. Die im Refinement geforderten Mechanismen werden wie folgt umgesetzt:

---

62 [assignment: *list of objects*]

63 [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*]]

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

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

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

- Eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) mit kryptographischen Verfahren beim Programmstart.
- Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K als Seed Quelle für den Zufallszahlengenerator des Betriebsystems (**OE.NK.RNG**).

Schutz von Geheimnissen, Seitenkanalresistenz

FPT_EMS.1/NK Emanation of TSF and User data

Dependencies: No dependencies.

FPT_EMS.1.1/NK The TOE shall not emit *sensitive data (as listed below) – or information which can be used to recover such sensitive data – through network interfaces (LAN or WAN)*[67] in excess of *limits that ensure that no leakage of this sensitive data occurs*[68] enabling access to

- *session keys derived in course of the Diffie-Hellman-Keyexchange-Protocol,*
- *[*none*]*[69]*,*
- *[*none*]*[70]*,*
- *[*none*]* [71]*,*
- *[*none*]* [72],
- [*none*][73] and
- *data to be protected (“*zu schützende Daten der TI und der Bestandsnetze”)
- [*none*][74].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)*[75] are unable to use the following interface *WAN interface or LAN interface of the connector*[76] to gain

---

67 [assignment: *types of emissions*]

68 [assignment: *specified limits*]

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

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

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

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

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

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

75 [assignment: *type of users*]

76 [assignment: *type of connection*]

access to **the sensitive data (TSF data and user data) listed above**[77].

Anwendungshinweis 93: Es wurden keine weiteren Verfeinerungen vorgenommen. Zur Integritätsprüfung beim Selbsttest und beim Software-Update werden öffentliche Schlüssel verwendet. Die Software Images werden unverschlüsselt übertragen. Die Authentisierung des Administrators wird vom Netzkonnektor durchgeführt. Für die entsprechenden Auswahl Operationen des NK-PPs [17] wurde daher „none“ gewählt.

Sicherheits-Log

FAU_GEN.1/NK.SecLog Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

hier erfüllt durch: FPT_STM.1/NK

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

b) All auditable events for the [not specified][78] level of audit; and

c)

- *start-up, shut down and reset (if applicable) of the TOE*
- *VPN connection to TI successfully / not successfully established,*
- *VPN connection to SIS successfully / not successfully established,*
- *TOE cannot reach services of the transport network,*
- *IP addresses of the TOE are undefined or wrong,*
- *TOE could not perform system time synchronisation within the last 30 days,*
- *during a time synchronisation, the deviation between the local system time and the time received from the time server exceeds the allowed maximum deviation (see refinement to FPT_STM.1*/NK*);*
- *changes of the TOE configuration.*[79]
- **Fehlerzustände according to [27], table 3**.[80]

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

---

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

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

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

[80] Refinement: Addition of “**Fehlerzustände according to [27], table 3“** to the list of auditable events

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

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

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

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

Anwendungshinweis 94: Es werden alle Fehlerzustände die in der Konnektor-Spezifikation [27], Abschnitt 3.3, Tabelle 3 aufgeführt sind protokolliert. Die Konnektor-Spezifikation fordert die Initialisierung des Protokollierungsdienstes und weiterer Dienste in der Boot-Phase und die Meldung des Abschlusses der Boot-Phase durch den Event "BOOTUP/ BOOTUP_COMPLETE". Der Protokollierungsdienst wird als erster Dienst gestartet wird, dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „start-up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet. Der Protokollierungsdienst als letzter Dienst bei einem Shut-down des EVG beendet wird, dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „shut down“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet.

Anwendungshinweis 95: Die benötigte Größe des für das Security Log zu reservierenden Speicherbereichs ist abhängig von der Größe der einzelnen Log-Einträge, von der verwendeten Kodierung und weiteren Produkteigenschaften. Die Hardware des Konnektors muss mindestens 16 GByte Speicher besitzen damit nebem den Software Anteilen von NK und AK ausreichend speicher für Protokolldaten zur Verfügung steht, siehe 1.3.6.

FAU_GEN.2/NK.SecLog User identity association

Dependencies: FAU_GEN.1 Audit data generation

hier erfüllt durch: FAU_GEN.1/NK.SecLog

FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

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

Anwendungshinweis 96: Der EVG nimmt bei Konfigurationsänderungen durch einen authentisierten Administrator die Identität (Identifikator) des ändernden Administrators in das Sicherheits-Log auf. Es werden keine unterschiedlichen Administrator-Rollen unterstützt.

6.2.6. Administration

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

FMT_SMR.1./NK Security roles

Dependencies: FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

FMT_SMR.1.1/NK The TSF shall maintain the roles

- *Administrator*,
- *SIS,*
- *TI*
- *Anwendungskonnektor*[81].

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

Refinement: Die TSF erkennen die in FMT_SMR.1.1 definierte Rolle Administrator daran, dass das Sicherheitsattribut „Autorisierungsstatus“ des Benutzers „Administrator“ den Wert „autorisiert“ besitzt.

Anwendungshinweis 97: Der EVG unterstützt die Rolle Administrator. Als Sicherheitsattribut „Autorisierungsstatus“ des Benutzers „Administrator“ wird das Identifikator-Attribut verwendet. Die Autorisierung wird vom Netzkonnektor duchgeführt. Bei erfolgreicher Autorisierung des Administrator wird das Attribut im EVG gesetzt.

Anwendungshinweis 98: In einem Gesamtkonnektor kann der Administrator des Netzkonnektors auch als NK-Administrator bezeichnet werden. – Externe vertrauenswürdige IT-Systeme wie Kartenterminals sind keine Rollen, also ohne Einfluss auf FMT_SMR.1./NK. Lediglich der Anwendungskonnektor wurde hier formal als Rolle definiert, da er das Sicherheitsverhalten von Funktionen des EVG steuern kann, siehe FMT_MOF.1/NK.TLS. Die Rollen SIS und TI werden nur im Zusammenhang mit den Paketfilterregeln für die Kommunkation mit deren VPN-Konzentratoren verwendet.

FMT_MTD.1/NK Management of TSF data

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

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

FMT_MTD.1.1/NK The TSF shall restrict the ability to [change_default, query, modify, [*activate/deactivate VPN*]]][82] the *real time clock, packet filtering rules* [*none*][83] to *the role Administrator*[84].

Refinement: Die *real time clock* bezieht sich auf die von OE.NK.Echtzeituhr geforderte Echtzeituhr. Obwohl die Echtzeituhr in der Umgebung liegt, wird ihre Zeit vom EVG genutzt und der EVG beschränkt den Zugriff (*modify* = Einstellen der Uhrzeit) auf diese Echtzeituhr. Die *packet filtering rules* legen das Verhalten des Paketfilters (O.NK.PF_LAN, O.NK.PF_WAN) fest.

Anwendungshinweis 99: Nur Administratoren dürfen administrieren: Die aufgelisteten administrativen Tätigkeiten können nur von Administratoren ausgeführt werden.

Anwendungshinweis 100: Nur der Administrator darf ein Deaktivieren der VPN-Verbindung vornehmen. Die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ wurde in die Liste bei FMT_SMF.1/NK aufgenommen und innerhalb von FMT_MTD.1/NK wurde der Zugriff auf diese Managementfunktion auf den Administrator beschränkt.

FIA_UID.1/NK.SMR Timing of identification

Identification of Security Management Roles

Dependencies: No dependencies.

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

- *all actions except for administrative actions (as specified by FMT_SMF.1/*NK*, see below)*[85]

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

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

Anwendungshinweis 101: Die Zuweisung all actions except for administrative actions (as specified by FMT_SMF.1/NK) aus dem NK-PP [17] wurde unverändert übernommen.

FIA_UAU.1/NK.SMR Timing of authentication

Authentication of Security Management Roles

Dependencies: FIA_UID.1 Timing of identification

---

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

83 [assignment: *list of TSF data*]

84 [assignment: *the authorised identified roles*]

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

Hier erfüllt durch: FIA_UID.1/NK.SMR

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

- *all actions except for administrative actions (as specified by FMT_SMF.1/*NK*, see below)*[86]

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

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

FTP_TRP.1/NK.Admin Trusted path

Trusted Path für den Administrator.

Dependencies: No dependencies.

FTP_TRP.1.1/NK.Admin The TSF shall provide a communication path between itself and [remote, local][87] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure][88].

FTP_TRP.1.2/NK.Admin The TSF shall permit [the TSF, local users, remote users][89] to initiate communication via the trusted path.

FTP_TRP.1.3/NK.Admin The TSF shall require the use of the trusted path for *initial user authentication and administrative actions*.[90]

Anwendungshinweis 102: Die Wartung erfolgt immer über die LAN-Schnittstelle (PS2). Lokale und entfernte Administration erfolgt dabei über getrennte Ports an der LAN-Schnittstelle. Der Remote Adminsitrator muss dazu Zugang zum lokalen Netz haben. Siehe dazu die entsprechende Beschreibung im Benutzerhandbuch [110]. Aus Sicht des EVG erfolgt der Zugand für remote user und local users Analog über eine TLS-gesicherte Verbindung gemäß FTP_ITC.1/NK.TLS und nach erfolgreicher Eingabe von Username und Passwort.

FMT_SMF.1/NK Specification of Management Functions

Dependencies: No dependencies.

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

---

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

87 [selection: *remote, local*]

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

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

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

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

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

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.)[91]

- **Aktivieren und Deaktivieren des VPN-Tunnels**[92]

Anwendungshinweis 103: Das Review (Lesen und Auswerten) der von FAU_GEN.1/NK.SecLog erzeugten Audit-Daten wird nicht als Managementfunktion modelliert.

FMT_MSA.1/NK.PF Management of security attributes

Nur der Administrator darf (gewisse) Filterregeln verändern.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

FMT_MSA.1.1/NK.PF The TSF shall enforce the *PF SFP*[93] to restrict the ability to [query, modify, [*change_default*]][94] the security attributes *packet filtering rules*[95] to *the roles „Administrator“,* [*no other authorised identified roles*][96].

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

– die Kommunikation zwischen dem Konnektor einerseits und dem Transportnetz, der Telematikinfrastruktur, sowohl

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

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

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

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

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

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

gesicherte als auch offene Fachdienste und zentrale Dienste, bzw. den Bestandsnetzen andererseits oder

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

betreffen, dürfen nicht über die Administrator-Schnittstelle verändert werden können. Der Administrator muss den gesamten WAN-seitigen Verkehr blockieren können (siehe Konnektorspezifikation [27], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [27], Kapitel 4.2.1.2, ANLW_FW_SIS_ADMIN_RULES) festlegen. Vorgabewerte dürfen nicht verändert werden („change-default“ ist nicht erlaubt).

Erläuterung: FMT_MSA.1/NK.PF sorgt als von FMT_MSA.3/NK.PF abhängige Komponente dafür, dass die Regeln für den Paketfilter (*packet filtering rules*, diese Regeln werden als security attributes angesehen) nur durch den Administrator oder eine andere kompetente Instanz (siehe FMT_SMR.1./NK) verändert werden können. Weiterhin legt die Konnektorspezifikation [27] fest, dynamisches Routing zu deaktivieren. Dies ist Gegenstand der Schwachstelleanalyse.

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

Anwendungshinweis 104: Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [27] definierten Anforderungen.

Anwendungshinweis 105: Der Administrator kann einzelne Filter-Regeln direkt über die Managment-Schnittstelle administrieren. Ebenso ist es möglich Filterregeln als signierte Regelsätze (XML Pakete) über die Managment-Schnittstelle zu übertragen. Die Signaturprüfung findet im EVG statt.

Anwendungshinweis 106: Der Netzkonnektor kann seine Filterregeln abhängig von Ereignissen des Anwendungskonnektors dynamisch anpassen. So gelten standartmäßig sehr restriktive Filteregeln, die zum Beispiel erst beim Aufbau eines VPN Kanals erweitert werden. Einstellungen der Filterregeln durch den Administrator werden dabei niemals überschrieben.

FMT_MSA.4/NK aus PP [17] ist für den EVG nicht relevant, da der EVG die Authentisierung des Administrators selbst durchführt, siehe O.NK.Admin_Auth und Anwendungshinweis 63:. Mit FIA_UAU.1/NK.SMR wurde eine die Authentisierung des Administrators modellierende Anforderung in das ST aufgenommen.

Anwendungshinweis 107: Nicht relevant

Software Update

Der EVG unterstützt das Software Update. Die fogenden SFRs wurden aus dem Protection Profile BSI-CC-PP-0098 [16] des Gesamtkonnektors abgeleitet.

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

Dependencies: FDP_ACF.1 Security attribute based access control
hier erfüllt durch: FDP_ACF.1/NK.Update

FDP_ACC.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][97] on
[

- *subjects:*
  (1) Administrator (S_Administrator)
  (2) Anwendungskonnektor (S_AK)
  (3) Netzkonnektor (S_NK)
- *objects:*
  (1) Update-Pakete
- *operations:*
  (1) Importieren
  (2) Verwenden

][98]

Operation	Beschreibung	Anmerkung
Importieren	Einlesen von bereitgestellten Update-Paketen und Aktualisieren der Komponenten des EVG.	Der Download kann automatisch erfolgen.

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

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

Verwenden	Die Update-Pakete werden zum Update der TSF-Daten, zum Update des EVG zu einem neuen EVG oder zum Update anderer externer Komponenten (eHealth-Kartenterminal) verwendet.	Das Installieren (Verwenden) des Updates kann automatisch erfolgen.

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

Dependencies: FDP_ACC.1 Subset access control

hier erfüllt durch: FDP_ACC.1/NK.Update

FMT_MSA.3 Static attribute initialisation

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

FDP_ACF.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][99] to objects based on the following:

[

- *subjects:*

(1) S_Administrator

(2) S_AK

(3) S_NK

- *objects:*

(2) Update-Pakete with security attributes:

a. *Signatur*

b. *Zulässige Software Version*

][100]

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

[

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

[100] [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*]

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

*(2) Die Subjekte S_Administrator, S_AK und S_NK dürfen nur Update-Pakete verwenden, die einer Firmwaregruppe angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist***, siehe Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM]**[101].

]**[102]**

FDP_ACF.1.3/NK.Update The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*]**[103]**.

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

[

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

]**[104]**

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

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_ACC.1/NK.Update

FMT_MSA.3

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

FDP_ITC.1.1/NK.Update The TSF shall enforce the *Update-SFP*[105] when importing user data, controlled under the SFP, from outside of the TOE.

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

---

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

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

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

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

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

FDP_ITC.1.3/NK.Update The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*Die TSF muss die Integrität und Authentizität der importierten Update-Dateien überprüfen.*][106]

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

Dependencies: FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_ACC.1/NK.Update

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

hier erfüllt durch: FDP_ITC.1/NK.Update

FDP_UIT.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][107] to [receive][108] user data ~~**in a manner**~~[109] protected from [modification, deletion, insertion][110]

FDP_UIT.1.2/NK.Update The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion][111] has occurred.

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

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

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

[109] refinement

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

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

6.2.7. Kryptographische Basisdienste

Anwendungshinweis 108: Die SFR der Familie FCS in CC Teil 2 [5] enthalten ein [assignment: *cryptographic algorithm*]. Diese Zuweisungen wurden in den SFR im PP [16] in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI bereits vorgenommen. Die TSF muss die darüberhinausgehenden verpflichtenden Vorgaben der angegebenen Standards soweit sie die angegebenen Algorithmen und Protokollen betreffen implementieren und darf den angegebenen Standards mit Ausnahme der zugewiesenen Kryptoalgorithmen nicht widersprechen. So fordert RFC 3602 die Unterstützung von AES 128 Bit, die Zuweisung des SFR FCS_COP.1/NK.ESP aber in Übereinstimmung mit der Spezifikation kryptographischer Algorithmen in der Telematikinfrastruktur [30] an seiner Stelle verbindlich den stärkeren AES 256 Bit. Die Zuweisung erfordert nicht, dass die TSF alle in den angegeben Standards zulässigen Optionen für die spezifizierten kryptographischen Operationen und Schlüsselmanagement-funktionen implementieren muss. Die Anforderungen an die Gewährleistung der Interoperabilität sind hiervon nicht betroffen.

Anwendungshinweis 109: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Dabei werden vom EVG auch HW Mechanismen (AES-NI) verwendet, sofern diese vom Administrator explizit ausgewählt werden.

FCS_COP.1/NK.Hash Cryptographic operation

Zu unterstützende Hash-Algorithmen

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1.1/NK.Hash The TSF shall perform *hash value calculation*[112] in accordance with a specified cryptographic algorithm *SHA-1, SHA-*

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

256, [none][113] and cryptographic key sizes *none*[114] that meet the following: *FIPS PUB 180-4 [54].*[115]

FCS_COP.1/NK.HMAC Cryptographic operation

Zu unterstützende Hash basierende MAC-Algorithmen

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.HMAC The TSF shall perform *HMAC value generation and verification*[116] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, [SHA-256]*[117] and cryptographic key sizes [*128 bit, 256 bit*] [118] that meet the following: *FIPS PUB 180-4 [54], RFC 2404 [62], RFC 4868 [63], RFC 7296 [60].*[119]

FCS_COP.1/NK.Auth Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

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

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

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

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

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

[117] [assignment: *cryptographic algorithm*]

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

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

EVG eingebracht, die Abhängigkeit wird inhaltlich durch FPT_TDC.1/NK.Zert erfüllt.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1.1/NK.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K storing the signing key and performing the RSA or ECC operation* [120]

in accordance with a specified cryptographic algorithm *ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpoolP256r1) and sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[121] and cryptographic key size *256 bit and 2048 bit*[122] that meet the following: *RFC 8017 (PKCS#1) [53], FIPS PUB 180-4 [54], Standard TR-03111 [23]*[123].

FCS_COP.1/NK.ESP Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.ESP The TSF shall perform *symmetric encryption and decryption with Encapsulating Security Payload*[124] in accordance with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42) or AES-GCM (OID 2.16.840.1.101.3.4.1.46 and OID 2.16.840.1.101.3.4.1.6)*[125] and cryptographic key sizes *128 bit and 256 bit*[126] that meet the

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

[121] [assignment: *cryptographic algorithm*]

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

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

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

[125] [assignment: *cryptographic algorithm*]

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

following: *FIPS 197 [55], RFC 3602 [61], RFC 4303 (ESP) [59], RFC 4106 [65], specification [30]* [127].

FCS_COP.1/NK.IPsec Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.IPsec The TSF shall perform *VPN communication*[128] in accordance with a specified cryptographic algorithm *IPsec-protocol*[129] and cryptographic key sizes *256 bit*[130] that meet the following: *RFC 4301 (IPsec) [56], specification [30]*[131].

FCS_CKM.1/NK Cryptographic key generation

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

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

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*key generation for IPsec Session Keys*][132] and specified cryptographic key sizes [*128 bit, 256 bit*][133] that meet the following: *specification [30], TR-03116 [19]*[134].

---

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

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

[129] [assignment: *cryptographic algorithm*]

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

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

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

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

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

Anwendungshinweis 110: Für alle mittels FCS_COP.1/... beschriebenen kryptographische Operationen (mit Ausnahme der Hashwertberechnung, siehe FCS_COP.1/NK.Hash) sind kryptographische Schlüssel erforderlich, die entsprechend der Abhängigkeiten von FCS_COP.1 aus CC Teil 2 [5] entweder durch eine Schlüsselgenerierung (FCS_CKM.1) oder durch einen Schlüsselimport (FDP_ITC.1 oder FDP_ITC.2) zu erfüllen sind. In diesem Security Target wurde entsprechend zum Schutzprofil NK-PP [17] eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols (bzw. Elliptic-curve Diffie–Hellman bei ECC) seine Sitzungsschlüssel (session keys) für die VPN-Kanäle ableitet; diese Ableitung wird als Schlüsselgenerierung angesehen. (Der Aspekt des Schlüsselaustausches mit einem VPN-Konzentrator wird als FCS_CKM.2/NK.IKE modelliert, siehe unten). Alle erzeugten Schlüssel besitzen mindestens 100 bit Entropie, damit der EVG resistent gegen Angriffe mit hohem Angriffspotential ist.

FCS_CKM.2/NK.IKE Cryptographic key distribution

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.2.1/NK.IKE The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *IPsec IKE v2*[135] that meets the following *standard: RFC 7296 [60], specifications [30], TR-02102-3 [18]*[136].

FCS_CKM.4/NK Cryptographic key destruction

Löschen nicht mehr benötigter Schlüssel.

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4.1/NK The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroisation*][137] that meets the following: [*none*][138].

---

135 [assignment: *cryptographic key distribution method*]

136 [assignment: *list of standards*]

137 [assignment: *cryptographic key destruction method*]

138 [assignment: *list of standards*]

Anwendungshinweis 111: FCS_CKM.4/NK zerstört die von den Komponenten FCS_COP.1/... sowie FCS_CKM.2 (FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE) benötigten Schlüssel. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle verwendeten Schlüssel. Die Schlüssel werden dabei mit Nullen überschrieben.

Anwendungshinweis 112: Die Operationen entsprechen den Anforderungen in den Dokumenten [19], [30] und [27]. Es wurden keine weiteren Verfeinerungen der Zuweisungen der Operationen durchgeführt. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle definierten Kryptoverfahren.
Der DH-Exponent für den Schlüsselaustausch weist eine Mindestlänge gemäß [30] auf (mindestens 256 Bit). Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy wurden die Vorgaben aus [30] berücksichtigt.

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Anmerkung 6. Die Absicherung der Administrationsschnittstellen des Netzkonnektors erfolgt mittels TLS. Die SFRs aus dem PP [17] wurden dafür entsprechend vervollständigt.

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

Grundlegende Sicherheitsleistungen eines TLS-Kanals

Dependencies: No dependencies.

FTP_ITC.1.1/NK.TLS The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and **is able to**[139] provide~~s~~ assured identification of its end points and protection of the channel data from modification **and**[140] disclosure.

FTP_ITC.1.2/NK.TLS The TSF **must be able to**[141] permit *the TSF or another trusted IT-Product*[142] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.TLS The TSF shall initiate communication via the trusted channel for *communication required by the Anwendungskonnektor, [for administration]*[143].

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von unbefugtem Löschen, Einfügen oder Wiedereinspielen von Daten während der Kommunikation. Der

---

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

[140] refinement (or → and)

[141] refinement (shall → must be able to)

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

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

Trusted Channel muss auf Basis des TLS-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [27] und [30], wobei TLS 1.2 gemäß RFC 5246 [69] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,

TLS_DHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Die Anforderung „assured identification" im ersten Element des SFR impliziert, dass der EVG in der Lage sein muss, die Authentizität des „trusted IT-product" zu prüfen. Im Rahmen dieser Überprüfung muss er in der Lage sein, eine Zertifikatsprüfung durchführen (siehe FPT_TDC.1/NK.TLS.Zert). Da allerdings der Anwendungskonnektor in Abhängigkeit von der TLS-Verbindung ggf. entscheiden kann, auf eine Authentisierung eines der Endpunkte zu verzichten, wurde ein entsprechendes refinement gewählt. Aus demselben Grund wurde dies für die Frage, ob der EVG selbst oder das andere IT-Produkt die Kommunikation anstoßen kann, durch ein refinement präzisiert, da auch dies vom Typ der TLS-Verbindung abhängt und vom Anwendungskonnektor entschieden wird.

Anwendungshinweis 113: Der EVG unterstützt TLS Version 1.2 (s. [30]). Der EVG unterstützt alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS, dabei werden die Anforderungen aus [30] erfüllt. Die Kryptosuiten werden für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt, sowie für die Absicherung der Administrationsschnittstellen. Der Konnektor unterstützt nicht TLS Version 1.0, 1.1 und SSL.

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

Prüfung der Gültigkeit von TLS-Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.TLS.Zert The TSF shall provide the capability to consistently interpret

(1) X.509-Zertifikate für TLS-Verbindungen

*(2) eine Liste gültiger CA-Zertifikate (**Trust-Service Status List TSL**)*

(3) Sperrinformationen zu Zertifikaten für TLS-Verbindungen, die via OCSP erhalten werden

(4) importierte X.509 Zertifikate für Clientsysteme

(5) eine im Konnektor geführte Whitelist von Zertifikaten für TLS-Verbindungen

(6) [no additional data types][144]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS.Zert The TSF shall use [*interpretation rules*][145] when interpreting the TSF data from another trusted IT product.

Refinement: Die „interpretation rules“ umfassen: Der EVG muss prüfen können, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist oder in einer gültigen Zertifikatskette bis zu einer zulässigen CA (Letzteres ggf. anhand der TSL) enthalten ist. Ebenso muss sie anhand einer OCSP-Anfrage prüfen können, ob das Zertifikat noch gültig ist.

Anwendungshinweis 114: Die *interpretation rules* orientieren sich an der Konnektor-Spezifikation [27].

Anwendungshinweis 115: Die **TSL** muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [27] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden. Der Konnektor kann die **TSL** bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [27]).

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

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

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

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

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

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

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384[146]
and specified cryptographic key sizes *128 bit for AES-128, 256 bit for AES-256, 160 for HMAC with SHA, 256 for HMAC with SHA-256 and 384 for HMAC with SHA-384*[147] that meet the following: *RFC 5246 [69]*.[148]

Anwendungshinweis 116: Der EVG unterstützt TLS Version 1.2 [38] (s. [30]). TLS 1.3 wird zurzeit nicht unterstützt. Der EVG unterstützt alle im SFR genannten cipher suites als Algorithmen für TLS. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [70]) bzw. dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (ECDHE_RSA nach [71]) oder ECC-Signaturen (ECDHE_ECDSA mit ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch die Kurven P-256 und P-384 (FIPS PUB 186-4 [108]) und die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. RFC-5639 [101] und RFC-7027 [109])). Die Auswahloperation zur Schlüssellänge hängt von den gewählten Algorithmen ab. Die Schlüssel werden für die TLS-Kommunikation zwischen dem EVG und anderen Komponenten genutzt. Es werden jeweils getrennte Schlüssel für jede Verwendung und Verschlüsselung nach FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.HMAC berechnet. Der EVG erzeugt Schlüssel mit einer Entropie von mindestens 100 Bit (siehe [19]). Bezüglich Diffie-Hellman-Gruppen für die Schlüsselaushandlung wurden die Vorgaben aus [30] beachtet. Der DH-Exponent für den Schlüsselaustausch weist eine Mindestlänge gemäß [30] auf. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange werden die gemäß [30] vorgegebenen Kurven unterstützt.

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

	Zu unterstützende Hash basierende MAC-Algorithmen
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or
	FDP_ITC.2 Import of user data with security attributes, or
	FCS_CKM.1 Cryptographic key generation]
	hier erfüllt durch: FCS_CKM.1/NK.TLS
	FCS_CKM.4 Cryptographic key destruction
	hier erfüllt durch: FCS_CKM.4/NK

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

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

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

FCS_COP.1.1/NK.TLS.HMAC The TSF shall perform *HMAC value generation and verification*[149] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[150] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[151] that meet the following: *Standards FIPS 180-4 [54] and RFC 2104 [75]*[152].

Anwendungshinweis 117: FCS_COP.1/NK.TLS.HMAC wird für die Integritätssicherung innerhalb des TLS-Kanals benötigt.

FCS_COP.1/NK.TLS.AES Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.AES The TSF shall perform *symmetric encryption and decryption*[153] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[154] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[155] that meet the following: *FIPS 197 [55], NIST 800-38D [99], RFC 5246 [69], RFC 8422 [100], RFC 5289 [72], specification [30]* [156].

Anwendungshinweis 118: Es gilt Anwendungshinweis 109.

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

[150] [assignment: *cryptographic algorithm*]

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

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

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

[154] [assignment: *cryptographic algorithm*]

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

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

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

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.Zert und FDP_ITC.2/NK.TLS.

Die *signature creation* wird im Standardfall von der gSMC-K bzw. SM-B durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K bzw. SM-B. In diesem Fall ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Neben der *verification of digital signatures* kann auch die *signatur creation* im EVG durchgeführt werden. Die entsprechenden privaten oder öffentlichen Schlüsselobjekte werden entweder im EVG erzeugt (FCS_CKM.1/NK.Zert) oder importiert (FDP_ITC.2/NK.TLS). Die Interpretation von TLS Zertifikaten wird durch FPT_TDC.1/NK.TLS.Zert erbracht.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1.1/NK.TLS.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K* **or SM-B**[157] *storing the signing key and performing the RSA* **and ECDSA**[158] *operation*[159]

c) signature creation with help of the FCS_CKM.1/NK.Zert and performing the RSA and ECDSA operation [160]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[161] **or ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpool256r1 or brainpool384r1)**[162] and cryptographic key sizes *2048 bit*[163] **or 384**

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

[158] Refinement: **and ECDSA**

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

[160] Refinement: **c) …**

[161] [assignment: *cryptographic algorithm*]

[162] Refinement: **or ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 (brainpool256r1)**

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

bit or 256 bit[164] that meet the following: *RFC 8017 (PKCS#1) [53], FIPS PUB 180-4 [54]*[165]*,* **Standard TR-03111 [23]**[166].

Anwendungshinweis 119: Die Signaturberechnung gemäß FCS_COP.1/NK.TLS.Auth wird für die Berechnung digitaler Signaturen zur Authentisierung bei TLS verwendet. Der EVG nutzt dafür bei Verbindungen ins lokale Netz (LAN) des Leistungserbringers die gSMC-K oder eine eigene Zertifikatsgenerierung bzw. ein importiertes Zertifikate/Schlüsselpaar (siehe FDP_ITC.2/NK.TLS). Im Fall der gSMC-K oder SM-B wird der dafür benötigte asymmetrische Schlüssel während der Produktion der gSMC-K oder SM-B importiert oder generiert. Es werden deshalb keine spezischen Anforderungen an die Quelle dieses Schlüssels gestellt. Für die asymmetrischen Schlüssel die im Konnektor generiert werden gilt FCS_CKM.1/NK.Zert. Für Verbindungen zum WAN wird eine SM-B verwendet die der Anwendungskonnektor ansteuert. Hier wird nur die LAN-seitige TLS-Verbindung modelliert. Die WAN-seitige TLS-Verbindung erfolgt analog und nutzt dieselben kryptografischen Basisdienste für TLS.

FCS_CKM.1/NK.Zert Cryptographic key generation / Certificates

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

nicht erfüllt mit folgender Begründung: FCS_CKM.1/NK.Zert bietet die Möglichkeit X.509 Zertifikate für die TLS-geschützte Kommunikation mit Clientsystemen zu erzeugen. Gemäß FDP_ETC.2/AK.Enc können die Zertifikate und die zugehörigen privaten Schlüssel vom Administrator exportiert werden. Keydistribution gemäß FCS_CKM.2 findet nicht statt.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK.Zert The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA Key Pair Generation, Elliptic Curve Key Pair Generation*][167] and specified cryptographic key sizes *2048 bit*[168] **for RSA and 256 bit for ECC with brainpoolP256r1**[169] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [52], BSI TR-03116-1 [19],*[170] **OID 1.2.840.10045.4.3.2, RFC 5639 [101], BSI TR-03111 [23]** [171]

---

[164] Refinement: **or 384 bit or 256 bit**

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

[166] Refinement: **Standard TR-03111 [23]**

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

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

[169] Refinement: **for RSA and 256 bit for ECC with brainpoolP256r1**

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

[171] Refinement: **OID 1.2.840.10045.4.3.2, RFC 5639 [101], BSI TR-03111 [23]**

The TSF shall

(1) create a valid X.509 [76] certificate with the generated RSA key pair and

(2) create a PKCS#12 [77] file with the created certificate and the associated private key. [172]

(3) create a valid X.509 [76] certificate with the generated ECDSA key pair[173]

Anwendungshinweis 120: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [30], Anforderung GS-A_4368 umsetzen. Die Verfeinerung zu FCS_CKM.1/NK.Zert soll die Möglichkeit zur Erzeugung von X.509 Zertifikaten für die TLS-geschützte Kommunikation mit Clientsystemen bieten. Die Zertifikate können für Clientsysteme oder den TOE verwendet werden, hierbei werden bei Clientzertifikate Schlüssel und Zertifikate exportiert und bei Serverzertifikaten nur die Zertifikate. Ein Export dieser Zertifikate ist Gegenstand von FDP_ETC.2/NK.TLS.

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

Import von Zertifikaten

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

Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanagt. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen importiert werden. Die Abhängigkeit wird durch FDP_ACC.1/AK.TLS des Anwendungskonnektors erfüllt.

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

hier erfüllt durch: FTP_TRP.1/NK.Admin

FPT_TDC.1 Inter-TSF basic TSF data consistency

hier erfüllt durch: FPT_TDC.1/NK.TLS.Zert

FDP_ITC.2.1/NK.TLS The TSF shall enforce the *Certificate-Import-SFP*[174] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/NK.TLS The TSF shall use the security attributes associated with the imported user data.

---

[172] refinement

[173] Refinement: **create a valid X.509 [76] certificate with the generated ECDSA key pair**

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

FDP_ITC.2.3/NK.TLS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/NK.TLS The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/NK.TLS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) Die TSF importiert X.509 Zertifikate für Clientsysteme durch den Administrator über die Management-Schnittstelle

(2) [Die TSF importiert X.509 Zertifikate und zugehörige private Schlüssel für den TOE durch den Administrator über die Management-Schnittstelle][175]

Anwendungshinweis 121: Gemäß FMT_MOF.1/NK.TLS überlässt der Netzkonnektor die Steuerung, unter welchen Umständen der Import von Client oder Server-Zertifikaten erfolgt, dem Anwendungskonnektor.

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

Export von Zertifikaten

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

Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanagt. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen erzeugt und exportiert werden. Die Abhängigkeit wird durch FDP_ACC.1/AK.TLS des Anwendungskonnektors erfüllt.

FDP_ETC.2.1/NK.TLS The TSF shall enforce the *Certificate-Export-SFP*[176] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/NK.TLS The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/NK.TLS The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/NK.TLS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) Die TSF exportiert X.509 Zertifikate für Clientsysteme und den zugehörigen privaten Schlüssel durch den

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

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

Administrator über die Management-Schnittstelle. Als Exportformat wird PKCS#12 verwendet.

(2) [Die TSF exportiert X.509 Zertifikate für Serversysteme durch den Administrator über die Management-Schnittstelle.][177]

Anwendungshinweis 122: Gemäß FMT_MOF.1/NK.TLS überlässt der Netzkonnektor die Steuerung, unter welchen Umständen der Export von Client- und Server-Zertifikaten erfolgt, dem Anwendungskonnektor.

FMT_MOF.1/NK.TLS Management of security functions behaviour

Management von TLS-Verbindungen durch den Anwendungskonnektor

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch FMT_SMF.1/NK

FMT_MOF.1.1/NK-TLS The TSF shall restrict the ability to determine the behaviour of[178] the functions *Management of TLS-Connections required by the Anwendungskonnektor*[179]to *Anwendungskonnektor*[180].

The following rules apply: For each TLS-Connection managed by the Anwendungskonnektor, only the Anwendungskonnektor can determine:

1. **Whether one or both endpoints of the TLS-connection need to be authenticated and which authentication mechanism is used for each endpoint.**
2. **Whether the Konnektor or the remote IT-Product or both can initiate the TLS-Connection.**
3. **Whether TLS 1.2 or TLS 1.3 (if provided) are used and which subset of the set of cipher suites as listed in FTP_ITC.1/NK.TLS is allowed for each connection.**
4. **Whether a "Keep-Alive" mechanism is used for a connection.**
5. **Which data can or must be transmitted via each TLS-Connection.**

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

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

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

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

6. **Whether the validity of the certificate of a remote IT-Product needs to be verified and whether a certificate chain or a whitelist is used for this verification.**
7. **Under which conditions a TLS-connection is terminated.**
8. **Whether and how terminating and restarting a TLS-connection using a Session-ID is allowed.**
9. **Whether and under which conditions certificates and keys for TLS-Connections are generated and exported or imported.**
10. **[*no additional rules*]**

If one or more of these rules are managed by the EVG itself, this shall also be interpreted as a fulfillment of this or these rules. [181]

Anwendungshinweis 123: Dieses SFR soll dafür sorgen, dass der Anwendungskonnektor alle Regeln durchsetzen kann, die gemäß der gematik-Spezifikationsdokumente für die verschiedenen vom Konnektor benötigten TLS-Verbindungen durchgesetzt werden müssen. Only TLS 1.2 is provided.

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

Erläuterung: Diese Regeln werden durch verschiedene SFRs des Anwendungskonnektor konkretisiert.

Anwendungshinweis 124: Es wurden keine SFRs aus dem Schutzprofil des Gesamtkonnektors [16] bezüglich Managment der TLS-Verbindungen auf den Netzkonnektor übertragen. Das Managment erfolgt durch den Anwendungskonnektor.

6.3. Funktionale Sicherheitsanforderungen des Anwendungskonnektors

6.3.1. Klasse FCS: Kryptographische Unterstützung

Der EVG implementiert kryptographische Algorithmen in der Software des Konnektors. Die asymmetrischen Algorithmen mit privaten Schlüsseln und die kryptographischen Algorithmen und Protokolle für die Kommunikation mit Chipkarten (d. h. dem HBA für Stapelsignatur und Komfortsignatur) werden in der gSMC-K (nicht Teil des EVG) implementiert. Die Ausnahme bildet die Verwendung eines X.509 Zertifikates (ID.AK.AUT) durch importiertes oder selbstgeneriertes Schlüsselmaterial. Die Software des Konnektors implementiert kryptographische Algorithmen und Protokolle für die IPsec-Kanäle und:

- Algorithmen für die Erstellung und die Prüfung elektronischer Signaturen, wobei die Erzeugung der digitalen Signaturen in den Chipkarten HBA und SMC-B als Träger der Signaturschlüssel genutzt werden,
- Algorithmen für die asymmetrische und symmetrische Verschlüsselung von Dokumenten,

[181] refinement

- Algorithmen für die symmetrische Entschlüsselung, wobei die asymmetrische Entschlüsselung der Dokumentenschlüssel in den Chipkarten erfolgt,
- Algorithmen für die MAC-Berechnung und die MAC-Prüfung (sowohl mit Blockchiffrieralgorithmen als auch mit Hashfunktionen) und
- Protokolle für die TLS-Verbindung mit den eHealth-Kartenterminals und die Kommunikation zwischen Fachmodulen und Fachdiensten.

Für alle Kryptoalgorithmen gelten die Festlegungen der TR-03116 [19] und der gematik-Spezifikation zu den anzuwendenden Kryptoalgorithmen [30].

Anwendungshinweis 125: Es gilt Anwendungshinweis 109

6.3.1.1. Basisalgorithmen

Der Konnektor nutzt kryptographische Dienste der gSMC-K, in der Einsatzumgebung.

Anmerkung 7. Für kartenbasierte Ver- und Entschlüsselung mit ECC gilt TAB_KON_747.

6.3.1.2. Schlüsselerzeugung und Schlüssellöschung

FCS_COP.1/AK.SHA	**Cryptographic operation / hash value calculation AK**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.SHA	The TSF shall perform *hash value calculation*[182] in accordance with a specified cryptographic algorithm *SHA-256, SHA-384 und SHA-512*[183] and cryptographic key sizes *none*[184] that meet the following: *Standard FIPS PUB 180-4 [54]*[185].

Anwendungshinweis 126: Die Hashfunktionen nach FCS_COP.1/AK.SHA werden durch den Signaturdienst benutzt.

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

[183] [assignment: *cryptographic algorithm*]

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

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

Anwendungshinweis 127: Die zu unterstützenden RSA-Verfahren unterscheiden sich zwischen QES und nonQES, da in letzterem Fall in der TI ausschließlich RSASSA-PSS Signaturen mit SHA-256 und Schlüssellängen von 2048 Bit vorkommen, während diese Einschränkungen für QES nicht gelten. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_CKM.1/AK.AES	**Cryptographic key generation / AES keys**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ AK.AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[***Random Number Generation for AES keys*]**[186]** and specified cryptographic key sizes *128 bit and 256 bit*[187] that meet the following: [*none*] [188].

Anwendungshinweis 128: Der EVG erzeugt Schlüssel mit einer Entropie von mindestens 100 Bit (siehe auch [19]). Dazu werden aus dem mit der gSMC-K geseedeten Zufallszahlengenerator des Betriebssystemkernels die entsprechende Anzhal von Bits entnommen. Nach [55] sind keine schwachen Schlüssel für den AES bekannt. Der EVG erzeugt alle Schlüsselbits durch den Zufallszahlengenerator gemäß der Einsatzumgebung, um eine maximale Entropie zu erreichen und keine Schwachstelle gegenüber der möglichen kryptographischen Stärke des AES zu bilden.

FCS_CKM.4/AK	**Cryptographic key destruction**
Hierarchical to:	No other components.
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_CMK.4.1/AK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroisation*][189] that meet the following: [*none*][190].

[186] [assignment: *Algorithm for cryptographic key generation **of AES keys***]

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

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

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

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

6.3.1.3. Signaturerzeugung und Signaturprüfung

Der EVG erzeugt aus den von den Chipkarten erzeugten digitalen Signaturen signierte Dokumente nach den angegeben Standards XAdES [82] [87], CadES [85] [88], PAdES [86] [89] und mit PKCS#1-Containern, PKCS#1v2.2, [90]. Der EVG prüft signierte Dokumente nach den angegebenen Standards und die bei der Stapelsignatur und der Komfortsignatur von den Chipkarten erzeugten digitalen Signaturen.

Anmerkung 8. Der Konnektor ermitteln bei der Signaturerstellung und Signaturprüfung (QES und nonQES) die Zertifikate und Schlüssel gemäß den Vorgaben in TAB_KON_900.

FCS_COP.1/AK.SigVer.SSA	**Cryptographic operation / Signature verification PKCS#1 SSA**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.SigVer.SSA	The TSF shall perform *verification of digital signatures*[191] in accordance with a specified cryptographic algorithm *RSASSA-PKCS1-v1_5 signature verification*[192] and cryptographic key sizes *1976 bit to 4096 bit*[193] that meet the following: *Standard PKCS#1 [90]*[194].

Anwendungshinweis 129: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.SSA wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet, wobei für die nonQES Signaturprüfung lediglich die Schlüssellänge 2048 Bit unterstützt wird. Die Verwendung von RSASSA-PKCS1-v1_5 für nonQES beschränkt sich auf die Prüfung von Zertifikaten, OCSP-Antworten sowie OCSP-Zertifikaten und wird nicht für die Prüfung von nicht-qualifizierten Dokumentensignaturen verwendet. [30]

Anwendungshinweis 130: Die zu unterstützenden RSA-Verfahren unterscheiden sich zwischen QES und nonQES, da in letzterem Fall in der TI ausschließlich RSASSA-PSS Signaturen mit SHA-256 und Schlüssellängen von 2048 Bit vorkommen, während diese Einschränkungen für QES nicht gelten. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signatur-erstellungszeitpunkt noch gültig waren.

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

[192] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/AK.SigVer.PSS	**Cryptographic operation / Signature verification PKCS#1 PSS**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.SigVer.PSS	The TSF shall perform *verification of digital signatures*[195] in accordance with a specified cryptographic algorithm *RSASSA-PSS signature verification*[196] and cryptographic key sizes *1976 bit to 4096 bit*[197] that meet the following: *Standard PKCS#1v2.2, [90]*[198].

Anwendungshinweis 131: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.PSS wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet, wobei für die nonQES Signaturprüfung lediglich die Schlüssellänge 2048 Bit unterstützt wird. [30]

Anwendungshinweis 132: Die zu unterstützenden RSA-Verfahren unterscheiden sich zwischen QES und nonQES, da in letzterem Fall in der TI ausschließlich RSASSA-PSS Signaturen mit SHA-256 und Schlüssellängen von 2048 Bit vorkommen, während diese Einschränkungen für QES nicht gelten. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_COP.1/AK.SigVer.ECDSA	**Cryptographic operation / Signature verification ECDSA**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.SigVer.ECDSA	The TSF shall perform *verification of digital signatures*[199] in accordance with a specified

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

[196] [assignment: *cryptographic algorithm*]

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

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

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

cryptographic algorithm *ECDSA*[200] and cryptographic key sizes *256 bit*[201] that meet the following: *Standard TR-03111 [23]*[202].

Anwendungshinweis 133: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.ECDSA wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet [30].

FCS_COP.1/AK.XML.Sign	**Cryptographic operation / XML signature generation**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.XML.Sign	The TSF shall perform *the generation of XML-signed documents*[203] **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm *(1) XML Advanced Electronic Signature (XAdES),* *(2) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS* *(3) SAML2-Token*[204] and cryptographic key sizes *no key*[205] that meet the following: *Standards SAML2.0 [101],XMLSig [80], XAdES[82] [87] and FIPS PUB 180-4 [54]*[206].

Anwendungshinweis 134: FCS_COP.1/AK.XML.Sign fordert die Erzeugung von XML-Signaturen nach vorgegebenen Signaturrichtlinien unter Nutzung der durch Chipkarten erzeugten digitalen Signaturen. Die Verfeinerung hebt hervor, dass bestimmte Anteile durch den EVG (insbesondere die Hashfunktion gemäß FCS_COP.1/AK.SHA) und andere Teile durch die Signaturchipkarten der Einsatzumgebung, insbesondere die Erzeugung der digitalen Signatur gemäß RSA mit RSA mit PKCS#1v2.2 PSS sowie ECDSA mit 256 Bit-Schlüsseln, geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel. Die Schnittstelle zur Signatur von SAML2-Token ist nur intern für Fachmodule nutzbar.

[200] [assignment: *cryptographic algorithm*]

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

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

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

[204] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/AK.CMS.Sign	**Cryptographic operation / CMS signature generation**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.CMS.Sign	The TSF shall perform *sign documents*[207] **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm *(1) CMS Advanced Electronic Signature (CadES),* *(2) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS* [208] and cryptographic key sizes *no key*[209] that meet the following: *Standards RFC5652 [78], CadES [85] [88] and FIPS PUB 180-4 [54]*[210].

Anwendungshinweis 135: FCS_COP.1/AK.CMS.Sign fordert die Erzeugung von CMS-Signaturen nach vorgegebenen Signaturrichtlinein. Die Verfeinerung hebt hervor, dass bestimmte Anteile durch den EVG (insbesondere die Hashfunktion gemäß FCS_COP.1/AK.SHA) und andere Teile durch die Signaturchipkarten der Einsatzumgebung, insbesondere die Erzeugung der digitalen Signatur gemäß RSA mit PKCS#1v2.2 RSASSA-PSS und RSA 2048 Bit-Schlüsseln sowie ECDSA mit 256 Bit-Schlüsseln, geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel.

FCS_COP.1/AK.PDF.Sign	**Cryptographic operation / PDF signature generation**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.PDF.Sign	The TSF shall perform *sign PDF-A documents*[211] **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm *SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS*[212] and

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

[208] [assignment: *cryptographic algorithm*]

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

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

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

[212] [assignment: *cryptographic algorithm*]

cryptographic key sizes *no key*[213] that meet the following: *Standards PAdES [86] [89] and FIPS PUB 180-4 [54]*[214] .

Anwendungshinweis 136: FCS_COP.1/AK.PDF.Sign fordert die Erzeugung von PDF-Signaturen. Die Verfeinerung hebt hervor, dass bestimmte Anteile durch den EVG (insbesondere die Hashfunktion gemäß FCS_COP.1/AK.SHA) und andere Teile durch die Signaturchipkarten der Einsatzumgebung, insbesondere die Erzeugung der digitalen Signatur gemäß RSA mit RSA mit PKCS#1 PSS und RSA 2048Bit-Schlüsseln sowie ECDSA mit 256 Bit-Schlüsseln, geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel.

FCS_COP.1/AK.XML.SigPr	**Cryptographic operation / XML signature verification**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.XML.SigPr	The TSF shall perform *verify signed XML documents*[215] in accordance with a specified cryptographic algorithm *(1) XML Advanced Electronic Signature (XAdES),* *(2) SHA-256, SHA-384 and SHA-512 for QES according to FCS_COP.1/AK.SHA with* *RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,* *RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES* [216] and cryptographic key sizes *1976 bit to 4096 bit for QES*[217], (3) *SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA*[218] and cryptographic key sizes *256 bit for QES*[219] that meet the following: *Standards XMLSig [1], XAdES [82] [87], FIPS PUB 180-4, PKCS#1[53], and TR-03111 [23]*[220].

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

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

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

[216] [assignment: *cryptographic algorithm*]

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

[218] [assignment: *cryptographic algorithm*]

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

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

Anwendungshinweis 137: FCS_COP.1/AK.XML.SigPr fordert die Prüfung von XML-Signaturen nach vorgegebenen Signaturrichtlinien und den bereits oben spezifizierten Kryptoalgorithmen. Die Prüfung von nonQES XAdES Signaturen ist nicht gefordert und wird nicht umgesetzt. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_COP.1/AK.CMS.SigPr	**Cryptographic operation / CMS signature verification**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.CMS.SigPr	The TSF shall perform *verify signed CMS documents*[221] in accordance with a specified cryptographic algorithm *(1) CMS Advanced Electronic Signature (CadES),* *(2) SHA-256, SHA-384 and SHA-512 for QES and SHA-256 for nonQES according to FCS_COP.1/AK.SHA with* *RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,* *RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES and nonQES*[222] and cryptographic key sizes *1976 bit to 4096 bit for QES and 2048 Bit for nonQES*[223], (3) *SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA*[224] and cryptographic key sizes *256 bit for QES and nonQES*[225] that meet the following: *Standards RFC5652[78], CadES [85] [88], FIPS PUB 180-4, PKCS#1 [53], and TR-03111 [23]*[226].

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

[222] [assignment: *cryptographic algorithm*]

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

[224] [assignment: *cryptographic algorithm*]

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

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

Anwendungshinweis 138: FCS_COP.1/AK.CMS.SigPr fordert die Prüfung von CMS-Signaturen nach vorgegebenen Signaturrichtlinein und den bereits oben spezifizierten Kryptoalgorithmen. Die zu unterstützenden RSA-Verfahren unterscheiden sich zwischen QES und nonQES, da in letzterem Fall in der TI ausschließlich RSASSA-PSS Signaturen mit SHA-256 und Schlüssellängen von 2048 Bit vorkommen, während diese Einschränkungen für QES nicht gelten. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_COP.1/AK.PDF.SigPr	**Cryptographic operation / PDF signature verification**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.PDF.SigPr	The TSF shall perform *verify signed PDF-A documents*[227] in accordance with a specified cryptographic algorithm *(1) PAdES [86] [89],* *(2) SHA-256, SHA-384 and SHA-512 for QES and SHA-256 for nonQES according to FCS_COP.1/AK.SHA with* *RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,* *RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES and nonQES*[228] and cryptographic key sizes *1976 bits to 4096 bits for QES and 2048 Bit for nonQES*[229], (3) *SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA*[230] and cryptographic key sizes *256 bit for QES and nonQES* [231] that meet the following: *Standards PAdES [86] [89], FIPS PUB 180-4, PKCS#1 [53] and TR-03111 [23]*[232].

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

[228] [assignment: *cryptographic algorithm*]

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

[230] [assignment: *cryptographic algorithm*]

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

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

Anwendungshinweis 139: FCS_COP.1/AK.PDF.SigPr fordert die Prüfung von PDF-Signaturen nach vorgegebenen Signaturrichtlinein und den bereits oben spezifizierten Kryptoalgorithmen. Die zu unterstützenden RSA-Verfahren unterscheiden sich zwischen QES und nonQES, da in letzterem Fall in der TI ausschließlich RSASSA-PSS Signaturen mit SHA-256 und Schlüssellängen von 2048 Bit vorkommen, während diese Einschränkungen für QES nicht gelten. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

Anwendungshinweis 140: Dieser Anwendungshinweis ist leer.

6.3.1.4. Ver- und Entschlüsselung von Dokumenten

FCS_COP.1/AK.AES	**Cryptographic operation / AES encryption and decryption**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.AES	The TSF shall perform *symmetric encryption and decryption* [233] in accordance with a specified cryptographic algorithm *AES-GCM*[234] and cryptographic key sizes *128 bit, 192 bit and 256 bit*[235] that meet the following: *Standards FIPS 197 [55], NIST-SP-800-38A [91],* ***NIST-SP-800-38D [92]*** [236].

Anwendungshinweis 141: FCS_COP.1/AK.AES wird u.a. für die symmetrische Verschlüsselung und Entschlüsselung von Dokumenten gemäß FCS_COP.1/AK.XML.Ver bzw. FCS_COP.1/AK.XML.Ent, FCS_COP.1/AK.CMS.Ver, bzw. FCS_COP.1/AK.CMS.Ent benötigt. Die Schlüssellängen 128 Bit und 192 Bit werden lediglich für die Entschlüsselung unterstützt. Man beachte, dass AES CBC nur noch für Secure Meassaging der Chipkarten und für TLS-Kanäle des Konnektors verwendet wird.

FCS_COP.1/AK.XML.Ver	**Cryptographic operation / XML encryption**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.XML.Ver	The TSF shall perform *encryption of XML documents in a hybrid cryptosystem*[237] in accordance with a specified cryptographic algorithm **ECIES and**[238] *RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit*[239] and cryptographic key sizes **256 bit for ECC,**[240] *256 bit for AES and 2048 bit for RSA*[241] that meet the following: *Standards*

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

[234] [assignment: *cryptographic algorithm*]

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

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

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

[238] Refinement: **ECIES and**

[239] [assignment: *cryptographic algorithm*]

[240] Refinement: **256 bit for ECC,**

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

NIST-SP-800-38D [92], PKCS#1 [53], FIPS 197 [55] und XMLEnc [79][242]**, [gemSpec_Krypt], Kap. 5.7**[243].

Anwendungshinweis 142: Dieser Anwendungshinweis ist im PP [16] leer und wird hier nur aufgeführt, um eine zum PP identische Nummerierung beizubehalten.

FCS_COP.1/AK.XML.Ent	**Cryptographic operation / XML decrpytion**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.XML.Ent	The TSF shall perform *decryption of XML documents in a hybrid cryptosystem*[244] in accordance with a specified cryptographic algorithm **ECIES and**[245] *[RSAOAEP]*[246] *and AES-GCM with authentication tag length of 128 bit*[247] and cryptographic key sizes **256 bit for ECC,**[248] 128 bit, 192 bit and *256 bit*[249] that meet the following: *Standards NIST-SP-800-38D [92], FIPS 197 [55] und XMLEnc [79]*[250]**, [gemSpec_Krypt], Kap. 5.7**[251].

Anwendungshinweis 143: Die asymmetrische Entschlüsselung des AES-Schlüssels mit privaten Schlüsseln gemäß [30] und [15] erfolgt durch die Chipkarte der Einsatzumgebung (HBA, SMC-B oder ggf. eGK).

Anwendungshinweis 144: Dieser Anwendungshinweis ist leer.

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

[243] Refinement: ECIES Standard hinzugefügt

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

[245] Refinement: **ECIES and**

[246] *[selection: RSA RSAES-PKCS1-v1_5, RSAOAEP]* (the selection was assigned in the PP)

[247] [assignment: *cryptographic algorithm*]

[248] Refinement: **256 bit for ECC,**

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

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

[251] Refinement: ECIES Standard hinzugefügt

Anwendungshinweis 145: Dieser Anwendungshinweis ist leer.

FCS_COP.1/AK.CMS.Ver	**Cryptographic operation / CMS encryption**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.CMS.Ver	The TSF shall perform *encryption of documents in a hybrid cryptosystem*[252] in accordance with a specified cryptographic algorithm **ECIES and**[253] *RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit*[254] and cryptographic key sizes **256 bit for ECC,**[255] *256 bit for AES, 256 bit for ECC and 2048 bit for RSA*[256] that meet the following: *Standards NIST SP800-38D [92], PKCS#1 [53], FIPS 197 [55] and CMS [78]*[257]**, [gemSpec_Krypt], Kap. 5.7**.[258]

Anwendungshinweis 146: Dieser Anwendungshinweis ist im PP [16] leer und wird hier nur aufgeführt, um eine zum PP identische Nummerierung beizubehalten.

FCS_COP.1/AK.CMS.Ent	**Cryptographic operation / CMS decryption**
Hierarchical to:	No other components.
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
FCS_COP.1.1/ AK.CMS.Ent	The TSF shall perform *decryption of documents in a hybrid cryptosystem*[259] in accordance with a specified cryptographic algorithm **ECIES and**[260] *[RSAOAEP]*[261] *and AES-GCM with*

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

[253] Refinement: **ECIES and**

[254] [assignment: *cryptographic algorithm*]

[255] Refinement: **256 bit for ECC,**

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

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

[258] Refinement: ECIES Standard hinzugefügt

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

[260] Refinement: **ECIES and**

[261] *[selection: RSA RSAES-PKCS1-v1_5, RSAOAEP]* (the selection was assigned in the PP)

authentication tag length of 128 bit[262] and cryptographic key sizes **256 bit for ECC,**[263] 128 bit, 192 bit and *256 bit*[264] that meet the following: *Standards NIST SP800-38D [92], PKCS#1 [53], FIPS 197 [55] and CMS [78]*[265]**, [gemSpec_Krypt], Kap. 5.7**[266].

6.3.2. Klasse FIA: Identifikation und Authentisierung

FIA_SOS.1/AK.Passwörter	**Verification of secrets / Passwords**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1/AK**.** Passwörter	The TSF shall provide a mechanism to verify that **administrator passwords** meet [*TIP1-A_4808 in [27]*][267].

Anwendungshinweis 147: Die Verfeinerung von „secrets“ zu „administrator passwords“ wurde durchgeführt, um die Qualitätsanforderungen gegenüber anderen Mechanismen abzugrenzen. Gemäß [27], Kap. 4.3.1, sind Administratorpasswörter gefordert, die den Anforderungen aus dem IT_Grundschutz-Katalog des BSI genügen.

FIA_SOS.2/AK.PairG	**TSF Generation of secrets / Pairing secret**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1/**AK.**PairG	The TSF shall provide a mechanism to generate **pairing** secrets that meet *the requirement to consist of 16 random bytes with 100 bit of entropy*[268].
FDP_SOS.2.2/**AK.**PairG	The TSF shall be able to enforce the use of TSF generated **pairing** secrets for *authentication of eHealth cardterminals*[269].

FIA_UID.1/AK	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/**AK**	The TSF shall allow

[262] [assignment: *cryptographic algorithm*]

[263] Refinement: **256 bit for ECC,**

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

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

[266] Refinement: ECIES Standard hinzugefügt

[267] [assignment: *a defined quality metric*]

[268] [assignment: *a defined quality metric*]

[269] [assignment: *list of TSF functions*]

*(1) Self test according to FPT_TST.1/AK**.Out-Of-Band**,*
(2) [Alternativer Werksreset und Werksreset für Fail Safe][270]
on behalf of the user to be performed before the user is identified.

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

Anwendungshinweis 148: Es wurde über das zugrundeliegende PP hinausgehend die Möglichkeit „Alternativer Werksreset und Werksreset für Fail Safe“ ohne vorherige Identifizierung durchzuführen.

FIA_UAU.1/AK	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1/**AK**	The TSF shall allow *(1) Identification of an user of the administrative interface, an user of the a Clientsytem, a smart cardand a eHealth cardterminal,* *(2) Signature verification according to **FDP_ACF.1/AK.SigPr**,* *(3) Encryption according to FDP_ACF.1/AK**.Enc**,* *(4) Handover of a card handle of an identified smart card,* *(5) [Alternativer Werksreset und Werksreset für Fail Safe]*[271] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/**AK**	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Anwendungshinweis 149: Der EVG erzwingt nur für die Administratorfunktion durch menschliche Nutzer sowie die Terminals und Chipkarten als technische Komponenten eine Authentisierung. Die TSF-vermittelten Aktionen zum Kartenmanagement, zur Signaturerstellung, zur Verschlüsselung und zur Entschlüsselung durch Benutzer des Clientsystems erfordern eine Autorisierung des Benutzers, d. h. seine erfolgreiche Authentisierung gegenüber der zu benutzenden authentisierten Chipkarte (für Signaturdienst gegenüber der Signaturchipkarte mit der PIN als Signaturschlüssel-Inhaber, für die Entschlüsselung gegenüber der Chipkarte mit dem Entschlüsslungsschlüssel als Kartenhalter als externe Komponenten der Einsatzumgebung. Es wurde über das zugrundeliegende PP hinausgehend die Möglichkeit „Alternativer Werksreset und Werksreset für Fail Safe“ ohne vorherige Authentisierung durchzuführen.

FIA_UAU.5/AK	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

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

FIA_UAU.5.1/AK The TSF shall provide

(1) [password based authentication mechanism][272] for administrator users,

(2) TLS authentication with a pairing secret for eHKT [27], TUC_KON_050,

(3) Asymmetric authentication of a smart card including CVC verification without negotiation of symmetric keys,

(4) Mutual asymmetric authentication with a smart card with CVC verification and negotiation of symmetric keys for a secure messaging channel[273]

(5) Authentication of the Clientsystem based on a User-ID with 128 bit length according to RFC 4122 [107]. For activation of the comfort signature mode the User-ID has to differ from the last 1000 User-IDs used for activation[274].

to support user authentication.

FIA_UAU.5.2/AK The TSF shall authenticate any user's claimed identity according to the *following rules:*

(1) The TSF shall authenticate the user for all administration functions.

(2) The TSF shall authenticate eHealth card terminals when establishing the TLS channel between the TSF and the eHealth card terminal.

(3) The TSF shall support the authentication of a eGK (identified by the ICCSN) with its smart card certificate.

(4) The TSF shall authenticate the HBA for a batch signature:

a. as a QSEE,

b. as a DTBS and PIN receiver before a signature creation process with negotiating symmetric keys for a secure messaging channel,

c. constantly during the signature process with secure messaging.

(5) The TSF shall authenticate the HBA before a single signature creation within the card session.

(6) *The TSF shall support mutual authentication in a remote PIN process: The gSMC-KT in the role of the PIN transmitter and the HBA (or the SMC-B) in the role of the PIN receiver[275].*

---

[272] *[selection: password based authentication mechanism, [assignment: another authentication mechanism]]* (The selection was assigned ion the PP)

[273] [assignment: *list of multiple authentication mechanisms*]

[274] Refinement: **(5) Authentication of the Clientsystem…**

[275] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

(7) The TSF shall authenticate the Clientsystem of the HBA-owner by means of the correct User-ID for a comfort signature

(8) The TSF shall authenticate the HBA for a comfort signature:

a. as a QSEE,

b. as a DTBS and PIN receiver before an activation of the comfort signatur mode with negotiating symmetric keys for a secure messaging channel,

c. constantly during the signature process with secure messaging.[276]

Anwendungshinweis 150: Eine Authentisierung einer KVK ist wegen der begrenzten Funktionalität der KVK nicht möglich. Die Card-to-Card-Authentisierung umfasst:

(1) einseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey,

(2) einseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey,

(3) gegenseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey,

(4) gegenseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey,

(5) gegenseitige asymmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals und

(6) gegenseitige symmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals.

wobei der Konnektor nur die Varianten (1) und (5) umsetzt.

Die Authentisierung von Chipkarten eGK, HBA und SMC-B gegenüber dem EVG schließt immer ein

(a) die Prüfung des CVC der Chipkarte, aus der die Authentisierungsreferenzdaten (öffentlicher Schlüssel) und die Rolle der Chipkarte hervorgeht, und

(b) das Kommando INTERNAL AUTHENTICATE an diese Chipkarte, deren Returncode durch den EVG geprüft wird.

Die CVC für die Authentisierung sind für die

a) die eGK in EF.C.eGK.AUT_CVC,

b) den HBA in EF.C.HPC.AUTR_CVC und EF.C.HPC.AUTD_SUK_CVC,

c) die gSMC-KT in EF.C.SMC.AUTD_RPS_CVC.E256 bzw. EF.C.SMC.AUTD_RPS_CVC.E384,

d) die SMC-B in EF.C.SMC. AUTD_RPE_CVC.E256

enthalten.

Die Unterstützung der gegenseitigen Authentisierung der gSMC-KT als PIN-Sender und des HBA bzw. der SMC-B als PIN-Empfänger in einem Remote-PIN-Prozess umfasst die Steuerung und die Kontrolle der gegenseitigen Authentisierung zur Aushandlung und Nutzung des Secure Messaging Kanals zwischen gSMC-KT und HBA bzw. SMC-B.

Das Kommando INTERNAL AUTHENTICATE kann dabei im Rahmen einer einseitigen oder gegenseitigen Authentisierung ausgeführt werden. Nur die Authentisierung durch Secure Messaging authentisiert über die unmittelbare Authentisierung durch INTERNAL AUTHENTICATE hinaus

[276] Refinement: **(7)** + **(8)**

(fortgesetzt) jedes Kommando und jede Antwort der Chipkarte. Im Fall der Einfachsignatur mit dem HBA im SE#1 ist der HBA unter Kontrolle des Benutzers lokal in PIN-Terminal gesteckt. Wenn die PIN-Eingabe und die Erstellung der digitalen Signatur zeitlich unmittelbar aufeinander folgen, genügt für diese Einfachsignatur eine einmalige (einseitige, symmetrische) Authentisierung des HBA als QSEE.

FIA_API.1/AK	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/AK	The TSF shall provide a *card-to-card authentication mechanism with key derivation for secure messaging*[277] to prove the identity of the *"SAK"*[278].

Anwendungshinweis 151: Diese SFR ergibt sich aus der TR-03114 [21] und den Zugriffsbedingungen des HBA, die für eine Stapelsignatur die Authentisierung der Identität „SAK" gegenüber dem HBA und die Übermittlung der DTBS mit Secure Messaging erfordern. Der EVG muss dafür über ein CVC mit der CHAT für die Identität „SAK" (vergl. C.SAK.AUTD_CVC in [33]) und die gSMC-K über den dazugehörigen privaten Schlüssel PrK.SAK.AUTD_CVC verfügen. Für eine Beschreibung des externen Verhaltens des EVG im Authentisierungsprotokoll mit dem HBA wird auf [21], [31], [35] und [33] verwiesen. Bei Aktivierung der Komfortsignatur ist die Authentisierung der Identität „SAK" gegenüber dem HBA, sowie bei der Durchführung von Komfortsignaturen die Übermittlung der DTBS mit Secure Messaging erforderlich (A_19258).

6.3.3. Klasse FDP: Schutz der Benutzerdaten

6.3.3.1. Zugriffskontrolldienst

Die Bezeichnungen TAB_KON_507 bis TAB_KON_514 beziehen sich auf Tabellen im Abschnitt 9.1 der vorliegenden Sicherheitsvorgaben, bzw. des zugrundeliegenden Schutzprofils.

FDP_ACC.1/AK.Infomod	**Subset access control / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK.Infomod	The TSF shall enforce the *Infomodell-SFP*[279] on *the subject S_Clientsystem, the objects as in TAB_KON_507, and the operation:*

[277] [assignment: *authentication mechanism*]

[278] [assignment: *identity or role*]

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

- *usage of the resource (the object) in a technical use case* [280].

FDP_ACF.1/AK.Infomod	**Security attribute based access control / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**Infomod	The TSF shall enforce the *Infomodell-SFP*[281] to objects based on the following: *the subject S_Clientsystem with its associated security attributes defined in Tabelle 14, and the objects with their associated security attributes defined in TAB_KON_508 and TAB_KON_509*[282].
FDP_ACF.1.2/**AK.**Infomod	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *TAB_KON_511, TAB_KON_512, TAB_KON_513 and TAB_KON_514.*[283]
FDP_ACF.1.3/**AK.**Infomod	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[284].
FDP_ACF.1.4/**AK.**Infomod	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[285].

FMT_MSA.1/AK.Infomod	**Management of security attributes / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles

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

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

[282] [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*]

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

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

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

	FMT_SMF.1 Specification of Management Functions.
FMT_MSA.1.1/**AK.**Infomod	The TSF shall enforce the *Infomodell-SFP*[286] to restrict the ability to modify, delete, create[287] the security attributes persistent entities and entity-connections *defined in TAB_KON_507, TAB_KON_508, TAB_KON_509 according to the contraints in TAB_KON_510*[288] to *S_Administrator*[289].

FMT_MSA.3/AK.Infomod	**Static attribute initialisation / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1/**AK.**Infomod	The TSF shall enforce the *Infomodell-SFP*[290] to provide [restrictive] [291] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/**AK.**Infomod	The TSF shall allow the *[no role]*[292] to specify alternative initial values to override the default values when an object or information is created.

6.3.3.2. Kartenterminaldienst

FDP_ACC.1/AK.eHKT	**Subset access control / Kartenterminaldienst**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

[286] [assignment: *access control SFP(s), information flow control SFP(s)*]

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

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

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

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

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

[292] *[Selection: S_Administrator, no role]* (the selection was assigned in the PP)

FDP_ACC.1.1/**AK.**eHKT

The TSF shall enforce the *Kartenterminaldienst-SFP*[293] on
subjects:
(1) *S_Kartenterminaldienst,*
(2) *S_Chipkartendienst,*
(3) *S_Signaturdienst,*
(4) *S_Verschlüsselungsdienst,*
(5) *S_AK,*
(6) *S_eHKT,*
(7) *S_Fachmodul,*
(8) *S_Clientsystem;*
objects:
(1) *eHealth-Kartenterminal,*
(2) *TLS-Kanal,*
(3) *SICCT-Kommando,*
(4) *Antwort auf SICCT-Kommando,*
(5) *Eingeschränkter Text;*
operations:
(1) *TLS-Kanal aufbauen,*
(2) *TLS-Kanal abbauen,*
(3) *Senden eines SICCT-Kommando anfordern,*
(4) *SICCT-Kommando senden.*
(5) *Antwort auf SICCT-Kommando empfangen;*
[294].

Operation	Beschreibung	Anmerkung
TLS-Kanal aufbauen	Aufbau des TLS-Kanals gemäß FTP_ITC.1/AK**.eHKT** mit gegenseitiger Authentisierung gemäß FIA_UAU.5/**AK**, Vereinbarung und Nutzung symmetrischer Schlüssel für Verschlüsselung AES und HMAC	Die TLS-Kanäle sind in [27] und [38] beschrieben. Die gesamte Kommunikation des Konnektors mit den eHealth-Kartenterminals erfolgt über die TLS-Kanäle des Kartenterminaldienstes.

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

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

Operation	Beschreibung	Anmerkung
	FCS_COP.1/NK.HMAC.	
TLS-Kanal abbauen	Freigabe der Resourcen des TLS-Kanals gemäß FDP_RIP.1/**AK** und Löschen der symmetrischen Schlüssel gemäß FCS_CKM.4/AK	Die eHealth-Kartenterminals setzen die gesteckten Chipkarten bei Abbau des TLS-Kanals zurück.
Senden eines SICCT-Kommando anfordern	Übergabe eines SICCT-Kommandos zur Übermittlung an eHealth-Kartenterminals	
SICCT-Kommando senden	Übermittlung eines SICCT-Kommandos gemäß [42] und [38]über den TLS-Kanal an ein eHealth-Kartenterminal,das durch den Chipkartendienst selbst erzeugt oder an den Kartenterminaldienst übergeben wurde	Die SICCT-Kommandos dienen [38] [42] - der Steuerung des eHealth-Kartenterminals, insbesondere zur Kommunikation mit dem Konnektor, Kommandoabarbeitung und Konfiguration der eHealth-Kartenterminals, - dem Zugriff auf die sichere Anzeige (Display und Anzeige des gesicherten PIN-Modus), und die Tastatur sowie ggf. dem Tongeber, - der Kontrolle, Aktivierung, Deaktivierung und Statusabfrage des elektrischen Zustands von Chipkartenkontaktiereinheiten und der Kommunikation mit Chipkarten in den Chipkartenslots, und - die Auslösung der Prozesse zur PIN-Eingabe und dem PIN-Wechsel im gesicherten Modus.
Antwort auf SICCT-Kommando empfangen	Empfangen der Antworten auf ein selbst gebildetes oder übergebenes SICCT-Kommando	

Tabelle 17: Operationen zur Zugriffskontrolle des Chipkartendienstes

FDP_ACF.1/AK.eHKT	**Security attribute based access control / Kartenterminaldienst**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**eHKT	The TSF shall enforce the *Kartenterminaldienst-SFP*[295] to objects based on the following: *list of subjects, objects and security attributes:* *subjects:* (1) *S_Kartenterminaldienst,* (2) *S_Chipkartendienst,* (3) *S_Signaturdienst,* (4) *S_Verschlüsselungsdienst,* (5) *S_AK with the security attributes:* a. *"Aufrufender: Clientsystem",* b. *"Aufrufender: Fachmodul"* (6) *S_eHKT,* (7) *S_Fachmodul,* (8) *S_Clientsystem;* *objects:* (1) *eHealth-Kartenterminal with security attribute „Arbeitsplatz",* (2) *TLS-Kanal,* (3) *SICCT-Kommando with security attribute „Typ des SICCT-Kommandos",* (4) *Antwort auf SICCT-Kommando* [296].
FDP_ACF.1.2/**AK.**eHKT	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only the Kartenterminaldienst may establish TLS-Kanäle to paired eHealth-Kartenterminals with mutual authentication.* *(2) Only the Kartenterminaldienst may shutdown TLS-Kanäle to eHealth-Kartenterminals. This is only allowed in case that communication errors have been detected.*

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

[296] [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*]

(3) *Only the Kartenterminaldienst may send SICCT-Kommandos and receive the associated reponses, which are used to control the eHealth-Kartenterminals (eHKT-Steuerungskommando).*

(4) *Only the Kartenterminaldienst and the Chipkartendienst may send SICCT-Kommandos and receive the associated reponses, which are used to access the secure display and the PIN pad of the eHealth-Kartenterminals (Benutzerkommuikations-kommando).*

(5) *The subject S_AK, calling subject = Fachmodul may*

- *pass SICCT-Kommandos to the Kartenterminaldienst which are used to display eingeschränkten Text on a identified eHealth-Kartenterminal and*
- *receive the associated reponses to the SICCT-Kommandos from the Chipkartendienst.*

(6) *Only the Chipkartendienst, the Signaturdienst and the Verschlüsselungsdienst may send SICCT-Kommandos via the TLS-Kanäle of the Kartenterminaldienst and receive the associated reponses, which are used to access inserted smart cards (Chipkartenkommando).*

(7) *Only the Chipkartendienst may send SICCT-Kommandos and receive the associated reponses, which are used for PIN entry, PUK entry and PIN change use cases in secure mode at the eHealth-Kartenterminals (PIN-Prozesskommando).*

(8) *Fachmodule and Clientsysteme may register themselves for the events „smart card inserted“ and „smart card removed“, to be notified if the events occur.*

.[297]

FDP_ACF.1.3/**AK.**eHKT The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *The S_Kartenterminal-dienst may establish a communication channel to an unpaired eHealth-Kartenterminal for the purpose of setup and pairing.*[298]

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

(1) *Only the subject S_Chipkartendienst may send a SICCT-Kommando via the TLS-Kanal of the TOE to the eHealth-Kartenterminal, which is used to display the messages „Signatur PIN“, „Signatur PUK“, „Freigabe PIN“, „Praxis PIN“, „Freigabe PUK“ oder „Praxis PUK“ at the eHealth-Kartenterminals.*

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

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

(2) *[none]* [299]
[300]

Die Zugriffskontrolle für die PIN-Authentisierung innerhalb eines logischen Kanals wird durch FDP_ACC.1/AK**.PIN** und FDP_ACF.1/AK**.PIN** beschrieben.

FDP_UCT.1/AK.TLS	**Basic data exchange confidentiality**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/**AK.**TLS	The TSF shall enforce the *Kartenterminaldienst-SFP*[301] to transmit and receive[302] ~~**user data**~~ **objects** in a manner protected from unauthorised disclosure.

FDP_UIT.1/AK.TLS	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1/**AK.**TLS	The TSF shall enforce the *Kartenterminaldienst-SFP*[303] to transmit and receive[304] user data ~~**in a manner**~~ protected from modification, deletion, insertion, replay[305] errors.
FDP_UIT.1.2/**AK.**TLS	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay[306] has occurred.

FMT_MTD.1/AK.eHKT_Abf	**Management of TSF data / eHealth-Kartenterminal Abfrage**
Hierarchical to:	No other components.

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

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

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

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

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

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

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

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

Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/**AK.**eHKT_Abf	The TSF shall restrict the ability to query and export[307] the *Arbeitsplatzkonfigurationsdaten:* *(1) Name eines zugelassenen eHealth-Kartenterminals,* *(2) Statische IP-Adresse eines zugelassenen eHealth-Kartenterminals,* *(3) Konfiguration des SICCT-Kommandointerpreter Ports eines eHealth-Kartenterminals,* *(4) Authentisierungsreferenzdaten mit Identität und Zertifikat der zugelassenen eHealth-Kartenterminals,* *(5) Zuordnung eines eHealth-Kartenterminals zum Arbeitsplatz,* *(6) Export von eHealth-Kartenterminal-Informationen*[308] to *S_AK and S_Administrator*[309]. **Pairing-Geheimnisse dürfen nur unter Wahrung der Vertraulichkeit exportiert und dürfen nicht abgefragt werden.**

FMT_MTD.1/AK.eHKT_Mod	**Management of TSF data / eHealth-Kartenterminal Modifikation**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/**AK.**eHKT_Mod	The TSF shall restrict the ability to modify, delete and import[310] the *Arbeitsplatzkonfigurationsdaten:* *(1) Name eines zugelassenen eHealth-Kartenterminals,* *(2) Statische IP-Adresse eines zugelassenen eHealth-Kartenterminals,* *(3) Konfiguration des SICCT-Kommandointerpreter Ports eines eHealth-Kartenterminals,*

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

[308] [assignment: *list of TSF data*]

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

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

(4) Authentisierungsreferenzdaten mit Identität und Zertifikat der zugelassenen eHealth-Kartenterminals,

(5) Zuordnung eines eHealth-Kartenterminals zum Arbeitsplatz

(6) Import von eHealth-Kartenterminal-Informationen nach Anzeige und Bestätigung

.[311]

to *S_Administrator*[312].

Anwendungshinweis 152: Die Iteration differenziert die Zugriffsbedingungen für das Management der Konfigurationsdaten nach Zugriffsarten und Rollen. Das Management der Kartenterminals ist in [27] beschrieben. FMT_MTD.1/eHKT_Abf definiert Sicherheitsanforderungen für den Export und FMT_MTD.1/eHKT_Mod für den Import von eHealth-Kartenterminal-Informationen wie in der Spezifikation Konnektor [27], Kap 4.3.3, beschrieben.

6.3.3.3. Chipkartendienst

FDP_ACC.1/AK.KD	**Subset access control / Chipkartendienst**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**KD	The TSF shall enforce the *Chipkartendienst-SFP*[313] on *subjects:* (1) *S_Chipkartendienst,* (2) *S_Signaturdienst,* (3) *S_Verschlüsselungsdienst,* (4) *S_AK,* (5) *S_Fachmodul,* (6) *S_Clientsystem;* *objects:* (1) *Chipkarte,* (2) *Logischer Kanal einer Chipkarte,* (3) *SICCT-Kommando with security attribute „Chipkartenkommando”;* *operations:* (1) *Kartenhandle ausgeben,* (2) *logischen Kanal anfordern,* (3) *logischen Kanal öffnen,* (4) *logischen Kanal schließen,*

[311] [assignment: *list of TSF data*]

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

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

(5) *die Card-to-card-Authentisierung anfordern,*
(6) *die Card-to-card-Authentisierung durchführen,*
(7) *Digitale Signatur erstellen,*
(8) *Chiffrate entschlüsseln,*
(9) *auf Kartenobjekte zugreifen,*
(10) *Chipkartenkommando übertragen und Antwort empfangen,*
(11) *Benutzerauthentisierung anfordern*
.[314]

Operation	Beschreibung	Anmerkung
Kartenhandle ausgeben	Für eine neu gesteckte Chipkarte wird ein eindeutiges Kartenhandle gebildet und an den EVG ausgegeben.	Die mit dem Kartenhandle verknüpften Informationen können folgende Sicherheits-attribute der Chipkarte enthalten: Identität des Kartenslots, Identität des eHealth-Kartenterminals, Identität des Arbeitsplatzes, dem das eHealth-Kartenterminal zugeordnet ist.
Logischen Kanal anfordern	Für eine mit dem Kartenhandle identifizierte Chipkarte wird ein logischer Kanal angefordert.	Der EVG kann mit einem Kartenhandle einen neuen logischen Kanal anfordern.
Logischen Kanal öffnen	Für eine mit dem Kartenhandle identifizierte Chipkarte wird ein logischer Kanal 1, 2 oder 3 geöffnet (Chipkartenkommando MANAGE CHANNEL).	Der EVG kann mit einem Kartenhandle einen neuen logischen Kanal anfordern.
Logichen Kanal schließen	Wenn der identifizierte logische Kanal der Kanal 0 ist, so ist der Sicherheitszustand dieses logischen Kanals zurückzusetzen. Wenn der identifizierte logische Kanal ein Kanal 1, 2 oder 3 ist, so ist der logische Kanal zu schließen (Chip kartenkommando MANAGE CHANNEL).	

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

Card-to-card-Authentisierung anfordern	Der EVG oder ein EVG-interner Dienst fordert die Card-to-Card-Authentisierung für zwei logische Kanäle verschiedener Chipkarten an	
Card-to-card-Authentisierung durchführen	Der EVG steuert die Card-to-card-Authentisierung für zwei logische Kanäle verschiedener Chipkarten.	
Digitale Signatur erstellen	Erstellen digitaler Signturen mit privaten Signaturschlüsseln und den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT und PSO: COMPUTE DIGITAL SIGNATURE.	Die Zugriffsregeln der Chipkarten entscheiden, ob das Kommando PSO: COMPUTE DIGITAL SIGNATURE für den kryptographischen Schlüssel zulässig ist.
Chiffrate entschlüsseln	Entschlüsseln von Chiffraten mit privaten Entschlüsselungsschlüsseln und den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT und PSO DECIPHER.	Die Zugriffsregeln der Chipkarten entscheiden, ob das Kommando PSO DECIPHER für den kryptographischen Schlüssel zulässig ist.
Auf Kartenobjekte zugreifen	Zugriff auf Datenobjekte der Chipkarten. Es wird zwischen lesendem und schreibenden Zugriff auf eine Datei bzw. Record, der Suche und dem Hinzufügen von Records unterschieden.	Die Chipkarten außer KVK verfügen über eine eigene Zugriffskontrolle auf Kartenobjekte.
Chipkarten-kommando übertragen und Antwort empfangen	Übertragung von Chipkarten-kommandos und das Empfangen von Antworten innerhalb von SICCT-Kommandos des Kartenterminal-dienstes	
Benutzerauthentisierung anfordern	Anforderung von Benutzerinteraktionen zur PIN-Authentisierung, PIN-Änderung, PIN-Entsperren, der Freischaltung einer SM-B durch einen HBA und die Abfrage des PIN-Status auslösen und die Rückantwort der Chipkarten zurückerhalten.	

Tabelle 18: Operationen zur Zugriffskontrolle des Chipkartendienstes

FDP_ACF.1/AK.KD	**Security attribute based access control / Chipkartendienst**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**KD	The TSF shall enforce the *Chipkartendienst-SFP*[315] to objects based on the following: *list of subjects, objects and security attributes:* *subjects:* (1) *S_Chipkartendienst,* (2) *S_Signaturdienst,* (3) *S_Verschlüsselungsdienst,* (4) *S_AK,* (5) *S_Fachmodul,* (6) *S_Clientsystem* *objects:* (1) *Chipkarte with security attributes:* *(a)„Kartentyp“,* *(b)„Kartenhandle“,* (2) *Logischer Kanal einer Chipkarte with security attribute „Sicherheitszustand“,* (3) *SICCT-Kommando with security attribute „Chipkartenkommando”* .[316]
FDP_ACF.1.2/**AK.**KD	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) *Der S_Chipkartendienst erzeugt für jede neu gesteckte Chipkarte ein Kartenhandle und übergibt für identifizierte eGK, SMC-B und HBA den im gespeicherten X.509 angegeben Namen des Kartenhalters an das Subjekt S_AK.* (2) *Die Subjekte S_AK und S_Fachmodul dürfen einen neu zuöffnenden logischen Kanal einer mit dem Kartenhandle identifizierten Chipkarte mit ggf. identifizierten User-ID, Clientsystem-ID, Arbeitsplatz anfordern. Wenn die übergebenen Identitäten mit der*

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

[316] [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*]

Arbeitsplatzkonfiguration konsistent sind und die identifizierte Chipkarte einen logischen Kanal bereitstellt, öffnet der Chipkartendienst einen solchen logischen Kanal und erlaubt den Zugriff auf die Chipkarte, wenn dem keine andere Zugriffsregel widerspricht

(3) *Der Signaturdienst und der Verschlüsselungsdienst dürfen einen neu zu öffnenden logischen Kanal einer mit dem Kartenhandle identifizierten Chipkarte anfordern. Wenn die die identifizierte Chipkarte einen logischen Kanal bereitstellt, öffnet der Chipkartendienst einen solchen logischen Kanal.*

(4) *Nur die Subjekte S_AK, S_Signaturdienst und S_Fachmodul dürfen die Card-to-Card-Authentisierung zwischen zwei logischen Kanäle verschiedener Chipkarten anfordern. Nur das Subjekt Chipkartendienst darf die Card-to-Card-Authentisierung für einen logische Kanäle durchführen.*

(5) *Nur der Signaturdienst darf mit den Chipkarten digitale Signaturen für QES und non-QES mit den Kommandos MANAGE SECURITY ENVIRONMENT und PSO COMPUTE DIGITAL SIGNATURE erzeugen.*

(6) *Nur der Verschlüsselungsdienst darf mit den Chipkarten Kommandos MANAGE SECURITY ENVIRONMENT und PSO DECIPHER auf Chipkarten zugreifen.*

(7) *Das Subjekt S_AK darf mit den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT, INTERNAL AUTHENTICATE, PSO COMPUTE DIGITAL SIGNATURE und GENERATE ASYMMETRIC KEY PAIR P1='81' auf den Schlüssel PrK.HCI.AUT zugreifen, wenn der Zugriff zu einem logischen Kanal einer SM-B gehört*

(8) *Nur der Chipkartendienst, der Signaturdienst, und der Verschlüsselungsdienst dürfen über einen logischen Kanal zu einer Chipkarte die Chipkartenkommandos MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE und MUTUAL AUTHENTICATE absetzen.*

(9) *Die Subjekte S_AK und S_Fachmodul, dürfen die Schließung des vom jeweiligen Subjekt angeforderten*

logischen Kanals anfordern. Der Chipkartendienst setzt den Sicherheitsstatus des logischen Kanals zurück.

(10) *Der Chipkartendienst löscht das Kartenhandle, wenn die betreffende Chipkarte gezogen wird.*

(11) *Fachmodule und Clientsysteme können sich für die Ereignisse „CARD INSERTED“, „CARD REMOVED“, „CARD PIN VERIFY_STARTED“, „CARD PIN VERIFY_FINISHED“, „CARD PIN CHANGE_STARTED“, „CARD PIN CHANGE_FINISHED“, "CARD PIN ENABLE_STARTED", "CARD PIN ENABLE_FINISHED", "CARD PIN DISABLE_STARTED" und "CARD PIN DISABLE_FINISHED" registrieren, um bei Eintritt der Ereignisse informiert zu werden.*

(12) *Das Clientssystem darf eine Benutzerauthentisierung anfordern.*[317]

FDP_ACF.1.3/**AK.**KD — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[318]

FDP_ACF.1.4/**AK.**KD — The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Kein Subjekt darf, wenn nicht ausdrücklich durch die Regeln in FDP_ACF.1.2 erlaubt, auf private und symmetrische Schlüssel der Chipkarten mit den Chipkartenkommandos MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE oder MUTUAL AUTHENTICATE zugreifen.

(2) Kein Subjekt darf auf DF.KT einer gSMC-KT zugreifen.

(3) Der EVG verhindert schreibenden Zugriff auf Kartenobjekte der KVK.

(4) [none] [319]

.[320]

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

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

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

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

Anwendungshinweis 153: Die Zugriffskontrolle für die PIN-Authentisierung innerhalb eines logischen Kanals wird durch FDP_ACC.1/AK**.PIN** und FDP_ACF.1/AK**.PIN** beschrieben. Die für die Fachmodule zulässigen Kommandos sind in der Spezifikation Konnektor [27], Kap. 4.1.5.4, definiert.

FDP_ACC.1/AK.PIN	**Subset access control / PIN**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**PIN	The TSF shall enforce the *VAD-SFP*[321] on *subjects* (1) *S_Chipkartendienst,* (2) *S_Signaturdienst,* (3) *S_Benutzer_Clientsystem,* (4) *PIN-Terminal,* (5) *S_eHKT,* (6) *S_eGK,* (7) *S_HBA,* (8) *S_HBAx,* (9) *S_gSMC-KT* (10) *S_SMC-B,* *objects:* (1) *Authentisierungsverifikationsdaten (VAD) as plaintext,* (2) *Authentisierungsverifikationsdaten (VAD) as ciphertext,* (3) *SICCT-Kommando* *operations:* (1) *lokale PIN-Eingabe anfordern,* (2) *lokale PIN-Eingabe durchführen,* (3) *entfernte PIN-Eingabe anfordern,* (4) *entfernte PIN-Eingabe durchführen,* (5) *VAD an Chipkarten senden,* (6) *VAD als Klartext verarbeiten,* (7) *VAD als Geheimtext verarbeiten,* (8) *VAD im Geheimtext ausgeben,* (9) *SICCT-Kommandos übertragen* .[322]

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

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

Operation	Beschreibung	Anmerkung
Lokale PIN-Eingabe anfordern	Anforderung der lokalen PIN-Eingabe unter Angabe der Chipkarte, der Funktion PIN-Prüfung, PIN-Wechsel oder PIN-Entsperren und der zu verwendende PIN- bzw. PUK-Referenz..	Der Begriff PIN-Eingabe kann die Eingabe der PIN, einer neuen Pin oder der PUK erfordern.
Lokale PIN-Eingabe durchführen	Steuern der lokalen PIN-Eingabe mit dem sicheren PIN-Modus des PIN-Terminals für eine gesteckte Chipkarte, der zu verwendende PIN-Referenz und der Funktion gemäß der Anforderung.	Die an den äußeren Schnittstellen sichtbaren Prozesse der lokalen PIN-Eingabe sind in [27], Kap. 4.1.5, beschrieben. Für HBA-VK wird nur die lokale PIN-Eingabe unterstützt.
Entfernte PIN-Eingabe anfordern	Anforderung der entfernten PIN-Eingabe unter Angabe des Arbeitsplatzes, der zu verwendenden Chipkarte, der Funktion PIN-Prüfung, PIN-Wechsel oder Anwendung der PUK und der zu verwendende PIN- bzw. PUK-Referenz.	Der Begriff PIN-Eingabe kann die Eingabe der PIN, einer neuen PIN oder der PUK erfordern.
Entfernte PIN-Eingabe durchführen	Steuern der entfernten PIN-Eingabe mit dem sicheren PIN-Modus des PIN-Terminals mit einer dort gesteckten gSMC-KT für eine Chipkarte in einem entfernten Chipkarten-Terminal, der zu verwendende PIN-Referenz, der Jobnummer zur Identifizierung des Signaturauftrags und des zu benutzenden PIN-Kartenterminals und der Funktion gemäß der Anforderung.	Die an den äußeren Schnittstellen sichtbaren Prozesse der entfernten PIN-Eingabe sind in [27], Kap. 4.1.5, und [21] beschrieben. Die entfernte PIN-Eingabe wird durch HBA-VK (HBAx mit dem Sicherheitsattribut HBA-VK) nicht unterstützt.
VAD an Chipkarte senden	Senden von SICCT-Kommandos an eHealth-Kartenterminals die VAD in den Chipkartenkommandos VERIFY, CHANGE REFERENCE DATA, DISABLE VERIFICATION REQUIREMENT, ENABLE	

	VERIFICATION REQUIREMENT und RESET RETRY COUNTER enthalten.	
VAD im Klartext verarbeiten	Lesen, Verarbeiten oder Ausgeben von unverschlüsselten VAD	
VAD im Geheimtext verarbeiten	Lesen, Verarbeiten oder Ausgeben von verschlüsselten VAD.	
VAD im Geheimtext ausgeben	Ausgeben von verschlüsselten VAD über die LAN-Schnittstelle.	
SICCT-Kommandos übertragen	Ein Subjekt sendet ein selbst gebildetes order entgegengenommenes (z. B. vom EVG zur Übertragung übergebenes) SICCT-Kommando an ein eHealth-Kartenterminal und verarbeitet die Antwort selbst oder gibt die Antwort an den Aufrufenden zurück.	Die SICCT-Kommandos sind in [42] und [38] beschrieben.

Tabelle 19: Operationen zur PIN-Eingabe

FDP_ACF.1/AK.PIN	**Security attribute based access control / PIN**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**PIN	The TSF shall enforce the *VAD-SFP*[323] to objects based on the following: *list of subjects, objects and security attributes:* *subjects:* (1) *S_Chipkartendienst,* (2) *S_Signaturdienst,* (3) *S_Fachmodul,* (4) *S_AK,* (5) *S_Benutzer_Clientsystem with security attribute Authorisierungsstatus,* (6) *PIN-Terminal with security attribute Authorisierungsstatus,* (7) *S_eHKT with security attribute Authorisierungsstatus,*

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

(8) *S_eGK mit dem Sicherheitsattribut CVC mit CHA, bzw. CHAT eGK,*

(9) *S_HBA mit dem Sicherheitsattribut CVC mit CHAT "PIN-Empfänger",*

(10) *S_HBAx mit Sicherheitsattribut „HBA" bzw. „HBA-VK",*

(11) *S_SMC-B mit dem Sicherheitsattribut CVC mit CHAT "PIN-Empfänger";*

objects:

(1) *Authentisierungsverifikationsdaten (VAD) as plaintext,*

(2) *Authentisierungsverifikationsdaten (VAD) as ciphertext,*

(3) *SICCT-Kommando*

.[324]

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

(1) *Das Subjekt S_AK, Fachmodule und das Clientsystem dürfen die lokale PIN-Eingabe und die entfernte PIN-Eingabe mit PIN-Referenz mit Ausnahme der Signatur-PIN und der Signatur-PUK für einen logischen Kanal einer Chipkarte beim Chipkartendienst anfordern.*

(2) *Das Subjekt „identifizierte Benutzer des Clientsystems" darf für die Signatur-PIN die lokale und entfernte PIN-Eingabe an seinem Arbeitsplatz für eine authentisierte Chipkarte zur PIN-Prüfung, zum PIN-Wechsel und zum Entsperren der PIN mit einer PUK anfordern.*

(3) *Das Subjekt Chipkartendienst darf die lokale PIN-Eingabe an authentisierten PIN-Terminal für jede identifizierte Chipkarte für alle PIN und PUK mit Ausnahme der Signatur-PIN und der Signatur-PUK durchführen.*

(4) *Das Subjekt Chipkartendienst darf die entfernte PIN-Eingabe an authentisierten PIN-Terminal mit einer authentisierten gSMC-KT als PIN-Sender für eine als PIN-Empfänger authentisierten HBA oder als PIN-Empfänger authentisierte SMC-B in einem authentisierten Chipkarten-Terminal für alle PIN und PUK mit Ausnahme der Signatur-PIN und der Signatur-PUK durchführen.*

(5) *Das Subjekt Signaturdienst darf die lokale PIN-Eingabe mit Signatur-PIN und Signatur-PUK am authentisierten PIN-Terminal für einen HBAx oder eine SMC-B für die PIN-Prüfung, den PIN-Wechsel oder PIN-Entsperren durchführen.*

[324] [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*]

(6) *Das Subjekt Signaturdienst darf die entfernte PIN-Eingabe mit der Signatur-PIN und der Signatur-PUK an authentisierten PIN-Terminals mit einer authentisierten gSMC-KT als PIN-Sender für eine als PIN-Empfänger authentisierten HBA oder als PIN-Empfänger authentisierte SMC-B in einem authentisierten Chipkarten-Terminal für die PIN-Prüfung, den PIN-Wechsel oder PIN-Entsperren durchführen.*

(7) *Die TSF steuert die PIN-Eingabe, so dass*

(a) wenn das PIN-Terminal und das Chipkarten-Terminal verschieden sind,

(i) ein gesicherter Kanal zwischen der gSMC-KT als PIN-Sender im PIN-Terminal und der Chipkarte als PIN-Empfänger im Chipkartenterminal vor der PIN-Eingabe aufgebaut wird,

(ii) das PIN-Terminal die eingegebene VAD im Klartext nur zum Verschlüsseln an die als PIN-Sender authentisierte gSMC-KT übergibt und nur die verschlüsselte VAD innerhalb des TLS-Kanals an den Konnektor übermittelt,

(iii) das Chipkartenterminal die verschlüsselte VAD nur für die PIN-Prüfung, das PIN-Entsperren oder den PIN-Wechsel dem als PIN-Empfänger authentisierten Heilberufsausweis oder der als PIN-Empfänger authentisierten SMC-B übergibt;

(b) wenn das PIN-Terminal und das Chipkarten-Terminal identisch sind, das PIN-Terminal die eingegebene VAD im Klartext nur für die PIN-Prüfung, PIN-Aktivierung, PIN-Deaktivierung, das PIN-Entsperren oder den PIN-Wechsel an die authentisierte eGK, den Heilberufsausweis und die SMC-B übergibt,

(c) *die PIN-Eingabe am PIN-Terminal nur im gesicherten Mode erfolgt.*[325]

FDP_ACF.1.3/**AK.**PIN The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*] [326]

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

(1) Kein Subjekt außer dem Chipkartendienst darf über den TLS-Kanal des EVG zu den eHealth-Kartenterminals SICCT-Kommandos mit dem Chipkartenkommando VERIFY, RESET RETRY COUNTER, DISABLE VERIFICATION

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

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

REQUIREMENT, ENABLE VERIFICATION REQUIREMENT oder CHANGE REFERENCE DATA absetzen.

(2) Kein Subjekt außer S_Fachmodul darf eine PIN-Eingabe zur PIN-Prüfung für eine eGK bei S_Chipkartendienst anfordern

(3) *[none]* [327]

[328]

Die durch **FDP_ACC.1/AK.PIN** und FDP_ACF.1/AK**.PIN** verwendeten Operationen sind in Tabelle 19 definiert.

Anwendungshinweis 154: Regel (2) in FDP_ACF.1.4/AK.PIN ist auch erfüllt, wenn der Aufruf nur indirekt über das Fachmodul erfolgt, also der direkte Aufruf bspw. vom Verschlüsselungs- oder Signaturdienst erfolgt, der Ursprung des Anwendungsfalls jedoch ein Fachmodul ist. Insbesondere die Abfrage der PIN der eGK über die Außenschnittstelle VerifyPin (vgl. [27]) durch das Clientsystem ist nicht gestattet.

6.3.3.4. Signaturdienst

FIA_SOS.2/AK.Jobnummer	**TSF Generation of secrets / Jobnummer**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1/**AK.**Jobnummer	The TSF shall provide a mechanism to generate **sechsstellige Jobnummern** ~~**secrets**~~ that meet *aus 3 zufälligen Großbuchstaben und 3 zufälligen Ziffern zu bestehen, wobei jedes Zeichen jeden Wert mit gleicher Wahrscheinlichkeit annimmt. Die TSF müssen sicherstellen, dass die letzten 1.000 vom EVG generierten Jobnummern einmalig sind* [329].
FIA_SOS.2.2/**AK.**Jobnummer	The TSF shall be able to enforce the use of TSF generated **sechsstellige Jobnummern** ~~**secrets**~~ for *Übergabe der Jobnummern ans Clientsystem* [330].

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

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

[329] [assignment: *a defined quality metric*]

[330] [assignment: *list of TSF functions*]

Anwendungshinweis 155: Die Verfeinerung von „Geheimnisse“ zu „sechsstellige Jobnummern“ ist notwendig, um den Ablauf der PIN-Eingabe zu konkretisieren. Die Jobnummer wird nach ISO646 DE aus den Bytes 0x30 bis x39 und x41 bis x5A angezeigt (s. [27], Kap. 4.1.8.1.3). Dies entspricht $1,76 \cdot 10^7$ möglichen Jobnummern. Laut [27] wird die Jobnummer vom Konnektor erzeugt und kann durch Clientsysteme abgerufen werden. Der Konnektor soll jedoch laut [27] keine Verbindung zwischen erzeugten und verwendeten Jobnummern herstellen. Die TSF sollen also nicht prüfen, ob nur Nummern verwendet werden, die vorher vom EVG erzeugt wurden, oder ob alle Nummern verwendet werden, die vom EVG erzeugt wurden.

FDP_ACC.1/AK.Sgen	**Subset access control / Signaturerstellung**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**Sgen	The TSF shall enforce the *Signaturerstellung-SFP*[331] on *subjects:* *(1) S_AK,* *(2) S_Signaturdienst,* *(3) S_Benutzer_Clientsystem;* *objects:* *(1) Zu signierende Dokumente,* *(2) Signaturstapel,* *(3) Signierte Dokumente;* *(4) Zu signierender Bitstring,* *(5) Signierter Bitstring;* *operations:* *(1) Signatur erstellen,* *(2) Signierte Dokumente erstellen,* *(3) Signatur mit der Signaturkarte erstellen,* *(4) Signaturvorgang abbrechen,* *(5) Signierte Dokumente zurückgeben,* (6) *Authentisierungsstatus der Signaturkarte zurücksetzen* .[332]

Operation	Beschreibung	Anmerkung

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

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

Signatur erstellen	Hashwerte zu signierender Dokumente berechnen, an die Signaturkarte zur Berechnung der digitalen Signatur senden und bei Empfang der digitalen Signatur von der Signaturkarte wird diese geprüft	Die Prüfung der digitalen Signatur stellt fest, ob die digitale Signatur für den übersandten Haswert und den vorgesehenen Signatur-schlüssel erzeugt wurde. Bei Übereinstimmung sind die Dokumente gültig signiert, sonst sind sie ungültig signiert.
Signierte Dokumente erstellen	Erzeugen einer oder mehrer signierter Dokumente gemäß FDP_DAU.2/QES	Für qualifizierte Signaturen erlaubt.
Signatur mit der Signaturkarte erstellen	Die DTBS wird an die Signaturkarte zur Berechnung der digitalen Signatur übergeben.	
Signaturvorgang abbrechen	Diese Operation unterbricht die Signatur eines Dokumentenstapels.	Der Konnektor MUSS jede Signaturerstellung für ein Dokumentenstapel unterbrechen können.
Signierte Dokumente zurückgeben	Die signierten Dokumente weden vom Signaturdienst an den Benutzer S_AK zur weiteren Verabeitung übergeben.	
Authentisierungsstatus der Signaturkarte zurücksetzen	Der Authentisierungsstatus der Signaturkarte wird zurücksetzt.	Nach Abarbeitung des Stapels, bei Abbbruch des Signaturvorgangs und bei festgestellten ungültig signierten Dokumente wird der Signatur-PIN-Authentisierungsstatus der Signaturkarte zurücksetzen.

Tabelle 20: Operationen zur Signaturerstellung

FDP_ACF.1/AK.Sgen	**Security attribute based access control / Signaturerstellung**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/**AK.**Sgen

The TSF shall enforce the *Signaturerstellung-SFP*[333] to objects based on the following *list of subjects, objects and security attributes:*

subjects:

(1) S_AK,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem with security attributes:

(a) „Identität des Benutzers“,

(b) „Authorisierungsstatus (HBA)“,

objects:

(1) Zu signierende Dokumente with security attributes:

(a) Authorisierungsstatus: „nicht autorisiert“,

(b) Authorisierungsstatus: „autorisiert“,

(c) Signaturrichtlinie,

(2) Signaturstapel,

(3) Signaturschlüssel externer Signaturchipkarten,

(4) Signierte Dokumente with security attributes:

(a) „ordnungsgemäß“

(b) „ungültig“

(5) Zu signierender Bitstring,

(6) Signierter Bitstring,

(7) Authentisierungsschlüssel von HBAx oder SM-B.

.[334]

FDP_ACF.1.2/**AK.**Sgen

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Das Subjekt S_AK darf nur nicht autorisierte zu signierende Dokumente an das Subjekt Signaturdienst übergeben und die zu verwendende Signaturrichtlinie, den Signierenden, den Arbeitsplatz und die Signaturkarte identifizieren.

(2) Nur das Subjekt S_Signaturdienst steuert den Signaturprozess des identifizierten Arbeitsplatzes.

(3) Das Subjekt S_Signaturdienst darf nur dann die zu signierenden Dokumente signieren, wenn

(a) der Sicherheitsstatus der Signaturchipkarte die Erzeugung der digitalen Signatur erlaubt.

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

[334] [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*]

(4) Wenn die identifizierte Signaturrichtlinie die Erzeugung einer qualifizierte elektronische Signatur fordert, dann

(a) muss das Subjekt S_AK den Signierenden und den Arbeitsplatz identifizieren,

(b) muss die identifizierte Signaturrichtlinie für eine qualifizierte elektronische Signatur geeignet sein,

(c) muss das Subjekt S_Signaturdienst für die Einfachsignatur die lokale Eingabe der QES-PIN an HBAx oder die entfernte Eingabe der QES-PIN an HBA steuern und für die Stapelsignatur die lokale oder entfernte PIN-Eingabe für HBA steuern,

(d) darf das Subjekt S_Signaturdienst nur für durch den HBA „autorisierten Benutzer des Clientsystems" zu signierenden Dokumente Signaturen mit der Signaturkarte erstellen, Signaturen ungültig signierter Dokumente sind zu löschen,

(e) das Subjekt S_Benutzer_Clientsystem darf den Signaturvorgang für die autorisierten zu signierenden Dokumente abbrechen,

(f) der S_Signaturdienst darf nur ordnungsgemäß signierte Dokumente an den S_AK zurückgeben,

(g) das Subjekt S_Signaturdienst muss nach Abarbeitung des Stapels, bei Abbbruch des Signaturvorgangs durch das Subjekt S_Benutzer_Clientsystem und bei festgestellten ungültig signierten Dokumente den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA zurücksetzen.

(h) das Subjekt S_Signaturdienst muss bei aktivierter Komfortsignatur nach Ablauf des Zählers SAK_COMFORT_SIGNATURE_MAX oder nach Ablauf der Zeit SAK_COMFORT_SIGNATURE_TIMER den Authentisierungsstatus der jeweiligen HBA-Kartensitzung zurücksetzten und bei Deaktivierung des Komfortsignatur-Modus SAK_COMFORT_SIGNATURE und bei Deaktivierung der Komfortsignatur durch die Operation DeactivtaeComfortSignature den Signatur-PIN-Authentisierungsstatus aller HBA-Kartensitzungen zurücksetzen.

(5) Wenn die gültige Signaturrichtlinie die Erstellung einer qualifizierten elektronischen Signatur verlangt, darf das Subjekt S_Signaturdienst nur ordnungsgemäße qualifizierte elektronische Signaturen an den S_AK zurück geben.

(6) *Das Subjekt S_AK darf dem S_Signaturdienst Binärstrings mit der maximalen Länge von 512 Bit ~~nur~~*[335] *zur Erstellung digitaler Signaturen mit Authentisierungsschlüsseln von HBAx oder SM-B übergeben und die von HBAx bzw. der SM-B signierte Binärstrings vom S_Signaturdienst empfangen.* [336]

FDP_ACF.1.3/**AK.**Sgen — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][337].

FDP_ACF.1.4/**AK.**Sgen — The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn der S_AK für die zu signierenden Dokumente eine Signaturrichtlinie zur Erstellung qualifizierter elektronische Signatur identifiziert, aber

(a) der Signierende keine qualifizierte elektronische Signatur erzeugen kann oder

(b) die Autorisierung des S_Benutzer_Clientsystem fehlschlägt.

(2) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn für diese zu signierenden Dokumente und den Signierenden die identifizierte Signaturrichtlinie ungültig ist.

(3) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für den Signaturstapel verweigern und alle für zu signierende Dokumente des Signaturstapels bereits erzeugten Signaturen löschen, wenn die Überprüfung der Signatur wenigstens einer signierten Datei des Signaturstapels fehlschlägt.

(4) Außer dem S_Signaturdienst darf kein Subjekt auf

(a) das Verzeichnis DF.QES des HBA,

(b) den Schlüssel PrK.HCI.OSIG der SMC-B,

(c) [none][338]

zugreifen.

---

[335] [refinement: ~~nur~~]

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

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

[338] [assignment: *weitere Signaturschlüssel externer Signaturchipkarten*]

(5) [none][339].

-[340]

Anwendungshinweis 156: Die Spezifikation Konnektor beschreibt die Schnittstelle zwischen dem Clientsystem und dem Konnektor zur Signaturerstellung und die Kartenhandle zur Identifikation einer gesteckten Chipklarte in Verbindung mit einem Arbeitsplatz des Benutzers. Der EVG kann die Signaturkarte des Signierenden mittels Kartenhandle identifizieren. Der EVG kann den Signierenden und den zu benutzenden Arbeitsplatz identifizieren.

Anwendungshinweis 157: Die Bedingungen für die Sicherheitsattribute signierter Dateien „ordungsgemäß“ und „ungültig“ sind durch FMT_MSA.4/**AK** festgelegt.

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

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

Anwendungshinweis 158: In PP-0098 wird das SFR FDP_ACF.1/AK.Sgen für die in dem PP beschriebenen Signaturarten „Einzelsignatur“ und „Stapelsignatur“ modelliert. Der EVG unterstützt zusätzlich die „Komfortsignatur“. Der Anwendungshinweis 158 des PP erlaubt ausdrücklich, dass für weitere Signaturarten teilweise von der Definition der SFR abgewichen werden kann. Insbesondere wird dabei FDP_ACF.1.2/AK.Sgen Regel (4)(g) genannt. Der EVG unterstützt zusätzlich die „Komfortsignatur“. Entsprechend wurde FDP_ACF.1/AK.Sgen um Regel (4)(f) erweitert. Die Komfortsignatur wird wie folgt umgesetzt (A_19102-04 und A_19103-06):
Wenn die Komfortsignatur für eine HBA-Kartensitzung aktiviert ist (SAK_COMFORT_SIGNATURE=enabled und Komfortsignatur-Modus aktiv) , wird der Authentisierungssatus der HBA-Kartensitzung erst dann zurückgesetzt, wenn eine konfigurierte Anzahl an einzelnen Signaturoperation durchgeführt wurde (SAK_COMFORT_SIGNATURE_MAX, Default=100, A_19100) oder ein konfigurierter Zeitwert abgelaufen ist (SAK_COMFORT_SIGNATURE_TIMER, Default=6h, A_18686-01). Der secunet konnektor 2.0.0 unterstützt bis zu zwei parallele HBA-Kartensitzungen für die Komfortsignatur. Die globalen Konfigurationswerte für das Aktivieren der Komfortsignatur-Funktionalität, für den Timer und für den Zähler können nur vom Administrator verwaltet werden (TIP1-A_4680-03). Für jede Kartensitzung werden vom Konnektor entsprechend der konfigurierten Werte für SAK_COMFORT_SIGNATURE_MAX und SAK_COMFORT_SIGNATURE_TIMER unabhängige Zähler und Timer verwaltet. Zudem wird der Authentisierungssatus aller HBAs bzw. HBA-Kartensitzungen bei Deaktivierung durch die Operation DeactiveComfortSignature oder direkt durch Deaktivierung des Komfortsignatur-Modus in der Managementoberfläche (SAK_COMFORT_SIGNATURE=disabled) zurückgesetzt.
Zudem wird bei Aktivierung der Komfortsignatur die übermittelte UserID auf Eindeutigkeit in Bezug auf die letzten 1000 Aufrufe (A_20074) und auf korrekte Länge (128 Bit) und Format RFC4122 geprüft (A_20073-01). Diese UserID ist als Authentisierungsgeheimnis zu behandeln und wird nicht vom Konnektor ausgegeben. Der TOE setzt entsprechend FDP_ACF.1.2/AK.Infomod (TIP1-A_4524-02) durch die Prüfung des Aufrufkontext durch, dass nur der Nutzer Komfortsignatur-Aufträge auslösen kann (SignDocument und TUC_KON_170), der die selbe UserID präsentiert, wie diese beim Aktivieren des Komfortsignatur-Modus für diese HBA-Kartensitzung (ActivateComfortSignature) präsentiert wurde. Schlägt die Prüfung fehl, wird die Operation abgebrochen. Die eigentliche Authentifizierung des Nutzers beim Auslösen der Komfortsignatur erfolgt außerhalb des TOE im Clientsystem. Es erfolgt ein entsprechender Hinweis im Handbuch bezüglich der Notwendigkeit und Bedeutung der Nutzer-Authentisierung, A_19101.
Weitere Signaturarten werden nicht im EVG umgesetzt.

FDP_ACC.1/AK.**SigPr** **Subset access control / Signature verification**

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/**AK.**SigPr The TSF shall enforce the *Signature verification-SFP*[341] on *subjects:*

(1) S_AK,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem;

objects:

(1) Signierte Dokumente,

(2) Signaturprüfungsergebnis;

operations:

(1) Signatur prüfen,

(2) Festlegen des angegebenen Zeitpunkts

[342] .

Operation	Beschreibung	Anmerkung
Signatur prüfen	Prüfung der digitalen Signatur mit Rückgabe der Prüfungsergebnisse and die aufrufende Instanz.	
Festlegen des angegebenen Zeitpunkts	Angabe des Zeitpunkts, der der Prüfung einer digitalen Signatur zugrundegelegt wird, wenn dieser in den signierten Dokumente fehlt oder von diesem abweichen soll.	Dies ist für die Prüfung qualifizierte elektronische Signaturen gefordert.

Tabelle 21: Operationen zur Signaturprüfung

FDP_ACF.1/AK.SigPr	**Security attribute based access control/ Signature verification**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**SigPr	The TSF shall enforce the *Signature verification-SFP*[343] to objects based on the following *list of subjects, objects and security attributes:* *subjects:*

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

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

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

(1) S_AK,
(2) S_Signaturdienst,
(3) S_Benutzer_Clientsystem;
objects:
(1) *Signierte Dokumente with the security attributes*
(a)Signaturrichtlinie,
(b)Angegebener Zeitpunkt,
(2) *Signaturprüfungsergebnis*
.[344]

FDP_ACF.1.2/**AK.**SigPr The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
(1) Das Subjekt S_AK darf signierte Dokumente an das Subjekt S_Signaturdienst zur Signaturprüfung übergeben und die Signaturrichtlinie identifizieren.
(2) Der Signaturdienst darf das Ergebnis der Signaturprüfung an das Subjekt S_AK zurückgeben.
[345].

FDP_ACF.1.3/**AK.**SigPr The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*]*[346]*.

FDP_ACF.1.4/**AK.**SigPr The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*]*[347]*.

Anwendungshinweis 159: Die signierten Daten enthalten in der Regel die Identität der Signaturrichtlinie und einen Zeitpunkt der Signaturerstellung. Die Signaturprüfung erfolgt nach der in den signierten Daten identifizierten Signaturrichtlinie. Die Auswahl des für die Signaturprüfung anzunehmenden Signaturzeitpunkts erfolgt entsprechend [27] hierarchisch:

- Für die QES-Signaturprüfung:
  - falls vorhanden Benutzerdefinierter_Zeitpunkt, sonst
  - falls vorhanden Ermittelter_Signaturzeitpunkt_Eingebettet, sonst
  - Ermittelter_Signaturzeitpunkt_System
- Für die nonQES-Signaturprüfung:
  - falls vorhanden Benutzerdefinierter_Zeitpunkt, sonst

[344] [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*]

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

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

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

- falls vorhanden Ermittelter_Signaturzeitpunkt_Eingebettet, sonst
- Ermittelter_Signaturzeitpunkt_System.

Bei der QES-Signaturprüfung ist die Auswertung von qualifizierten Zeitstempeln (Ermittelter_Signaturzeitpunkt_Qualifiziert) nach [27] optional. Ein gegebenenfalls vorhandener qualifizierter Zeitstempel wird vom Konnektor vollständig ignoriert.

FDP_DAU.2/AK.QES	**Data Authentication with Identity of Guarantor / Qualifizierte elektronische Signatur**
Hierarchical to:	FDP_DAU.1 Einfache Datenauthentisierung
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/**AK.**QES	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *data to be signed*[348] **durch qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der qualifizierten Signaturerstellungseinheit (QSEE) zur Erzeugung der digitalen Signatur**. **Es sind die Dokumentenformate zu signierender Daten** **(1) Text-Dateien (UTF-8 [95] oder ISO-8859-15 [93]),** **(2) TIFF-Dateien [94],** **(3) Adobe Portable Document Format (PDF/A) [96] [97],** **(4) XML-Dateien [98] [83]** **und die Formate signierter Daten** **(1) PAdES [86]** [**89**] **für PDF/A-Dokumente,** **(2) CadES [85] [88] für XML, PDF/A, Text und TIFF Dokumente,** **(3) XAdES [82] [87] für XML-Dokumente** **mit den Signaturvarianten** **(1) enveloped signature,** **(2) enveloping signature,** **(3) detached signature** **zu unterstützen.**
FDP_DAU.2.2/**AK.**QES	The TSF shall provide *S_Benutzern*[349] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence **durch qualifizierte elektronische Signatur in den in FDP_DAU.2.1/QES genannten Formaten sowie den Verfahren ECDSA [2] und PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [90]**.

[348] [assignment: *list of objects or information types*]

[349] [assignment: *list of subjects*]

Dies sind im einzelnen:

(1) ob die signierten Daten unverändert sind, d. h. das Ergebnis der Korrektheitsprüfung der digitalen Signatur über die signierten Daten,

(2) der der Signatur zuzuordnende Signaturschlüssel-Inhaber,

(3) die Inhalte des Zertifikates, auf dem die Signatur beruht,

(4) das Ergebnis der Nachprüfung der Zertifikate nach dem Kettenmodell, d. h. die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,

- **a. der angenommene Signaturerstellungszeitpunkt, wobei gegen folgende Zeitpunkte zu prüfen ist, sofern die Voraussetzungen durch die zu prüfenden Daten erfüllt sind:**
  - **i. vom Benutzer definierter Zeitpunkt, sonst**
  - **ii. in der Signatur eingebetteter Zeitpunkt, sonst**
  - **iii. [none],**
  - **iv. bzw. wenn diese nicht vorliegen der Jetzt-Zeitpunkt;**
- **b. das Vorhandensein des Zertifikats des VDA, der das Signaturzertifikat ausgestellt hat, in der BNetzA-VL.**
- **c. die Korrektheit der digitalen Signatur des Signaturzertifikats,**
- **d. die Anforderung von OCSP-Anfragen und die Auswertung von OCSP-Antworten, ob das nachgeprüfte qualifizierte Signaturzertifikat im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war.**

(5) Für jedes Ergebnis der Korrektheitsprüfung einer digitalen Signatur ist anzugeben, ob

- **a. die kryptographische Prüfung der digitalen Signatur mit dem dazugehörigen öffentlichen Schlüssel deren Korrektheit bestätigt hat oder nicht,**
- **b. die für die Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum angegeben Signaturerstellungszeitpunkt geeignet waren, wenn dies nicht der Fall ist, liegt keine qualifizierte elektronische Signatur vor;**
- **c. die für die Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum Signaturprüfzeitpunkt geeignet sind; wenn dies nicht der Fall ist, ist eine Information zum verminderten Beweiswert der qualifizierte elektronischen Signatur zurückzugeben.**

(6) **[*none*][350].**

Anwendungshinweis 160: Für den allgemeinen Begriff der Signaturrichtlinie sei auf die Ausführungen in Abschnitt 1.3.5.2 verwiesen. Die Verfeinerung des Elements FDP_DAU.2.1/QES durch die Ergänzung „mit Hilfe der qualifizierten Signaturerstellungseinheit zur Erzeugung der digitalen Signatur“ ist notwendig, da die digitale Signatur durch die qualifizierte Signaturerstellungseinheit (z. B. den HBA) erstellt wird. Die Spezifikation Konnektor [27] schränkt die zu unterstützenden Kombinationen der Dokumentenfromate, Formate signierter Daten und Signaturvarianten ein. Diese Einschränkungen gelten auch FDP_DAU.2.1. Die für die Prüfung der qualifizierten elektronischen Signatur notwendigen Angaben (wie z.B. Angaben zu dem der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikat) werden durch den EVG mit Hilfe der PKI-Dienste erstellt.

Die Identität des Benutzers, der den Nachweis generiert hat, wird aus dem der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikat abgeleitet. Dies kann ein Pseudonym sein.

Anwendungshinweis 161: Für die Prüfung der Zertifikate, der OCSP-Antworten und der OCSP-Zertifikate werden im QES-Bereich die selben Verfahren wie für die Prüfung der qualifizierten Dokumentensignaturen unterstützt.

Anwendungshinweis 162: Die Informationen aus dem OCSP-Dienst können eine gewisse Zeit in einem Cache gepuffert und verwendet werden. Dabei ist zu beachten, dass der verwendete Zeitpunkt der aus dem Cache entnommenen Prüfergebnisse nicht älter ist als der zu prüfende Signaturerstellungszeitpunkt. Der maximale Zeitraum der Verwendung des OCSP Cache kann vom Administrator vorgegeben werden.

Anwendungshinweis 163: Der Konnektor unterstützt die Signaturvariante „detached signature“.

FDP_DAU.2/AK.Sig	**Data Authentication with Identity of Guarantor / NonQES**
Hierarchical to:	FDP_DAU.1 Einfache Datenauthentisierung
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/**AK.**Sig	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *zu signierenden Daten*[351] **durch nicht-qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der Chipkarten**. **Es sind die Dokumentenformate zu signierender Daten** **(1) Text-Dateien (UTF-8 [95] oder ISO-8859-15 [93]),** **(2) TIFF-Dateien[94],** **(3) Adobe Portable Document Format (PDF/A) [96],** **(4) XML-Dateien [98] [83],**

[350] **[assignment: *andere Form von Nachweisen*]**

[351] [assignment: *list of objects or information types*]

(5) Binärdokument,

und die Formate signierter Daten

(1) PAdES [86] [89] für PDF/A-Dokumente,

(2) CadES [85] [88] für Text, TIFF, Adobe Portable Document Format (PDF/A) und XML Dokumente sowie Binärdokumente,

(3)

mit den Signaturvarianten

(1) enveloped signature,

(2) enveloping signature,

(3) detached signature

zu unterstützen.

FDP_DAU.2.2/**AK.**Sig The TSF shall provide *S_Benutzern*[352] with the ability to verify evidence of the validity of the indicated information ~~**and the identity of the user that generated the evidence**~~ **durch nicht-qualifizierte elektronische Signatur in den in FDP_DAU.2.1/Sig genannten Formaten sowie den Verfahren ECDSA [3], PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [90] gemäß gültiger Signaturrichtlinie**. **Dies sind im einzelnen:**

(1) ob die signierten Daten unverändert sind, d. h. das Ergebnis der Korrektheitsprüfung der Signatur,

(2) der Signatur zuzuordnende Signaturschlüssel-Inhaber,

(3) die Inhalte des Zertifikates, auf dem die Signatur beruht,

(4) das Ergebnis der Nachprüfung von Zertifikaten in der Zertifikatskette,

(5) die Anforderung von OCSP-Anfragen und die Auswertung von OCSP-Antworten,

[*none*][353]**.**

[352] [assignment: *list of subjects*]

[353] **[assignment: *andere Form von Nachweisen*]**

Anwendungshinweis 164: Der EVG unterstützt die Erzeugung und die Prüfung von nicht-qualifizierten elektronischen Signaturen. Dies können fortgeschrittene elektronische Signaturen oder digitale Signaturen sein. In beiden Fällen muss aber eine gültige Signaturrichtlinie vorliegen. Für Binärdokumente und Binärstrings werden keine Formatanforderungen gestellt. Die Verfeinerung des Elements FDP_DAU.2/AK**.Sig** durch die Ergänzung „mit Hilfe der Chipkarten“ ist notwendig, da die digitale Signatur durch eine nicht zum EVG gehörige Chipkarte (z. B. eine SMC-B) erstellt wird. Die anderen für die Prüfung der elektronischen Signatur oder einer digitalen Signatur notwendigen Angaben (wie z.B. Angaben zu dem der elektronischen Signatur zugrunde liegenden Zertifikat) werden durch den EVG erstellt. Zum Nachweis der erfolgreichen Prüfung werdendie für die Gültigkeitsprüfung benutzten OCSP-Antworten mit einem Zeitstempel versehen und dem Nutzer zugänglich gemacht. Es werden neben der NFDM-Signaturrichtlinie und dem in FDP_DAU.2/AK**.Sig** und im PP [15], Kapitel 1.3.5.2 beschriebenen Standardablauf zur Signaturprüfung keine weiteren Signaturrichtlinien unterstützt..

Anwendungshinweis 165: Die Informationen aus dem OCSP-Dienst können eine gewisse Zeit in einem Cache gepuffert und verwendet werden. Dabei ist zu beachten, dass der verwendete Zeitpunkt der aus dem Cache entnommenen Prüfergebnisse nicht älter ist als der zu prüfende Signaturerstellungszeitpunkt. Der maximale Zeitraum der Verwendung des OCSP Cache kann vom Administrator vorgegeben werden.

Anwendungshinweis 166: Das Verfahren sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) wird im nonQES-Bereich nur für die Prüfung der Zertifikate, der OCSP-Antworten und der OCSP-Zertifikate unterstützt, nicht jedoch für nicht-qualifizierte Dokumentensignaturen. Für die Prüfung der Zertifikate, der OCSP-Antworten und der OCSP-Zertifikate werden im nonQES-Bereich zudem die selben Verfahren wie für die Prüfung der nicht-qualifizierten Dokumentensignaturen unterstützt.

FDP_DAU.2/AK.Cert	**Data Authentication with Identity of Guarantor / Überprüfung von Zertifikaten**
Hierarchical to:	FDP_DAU.1 Einfache Datenauthentisierung
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/**AK.**Cert	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *Signaturen*[354].
FDP_DAU.2.2/**AK.**Cert	The TSF shall provide *S_Benutzern*[355] with the ability to verify evidence of the validity of the indicated **Zertifikatsprüfung, einschließlich Zertifikatsinhalt ~~information~~** and the identity of the user that generated the evidence. **Dies sind im einzelnen:** **(1) der Inhalt des Zertifikats, auf dem die Signatur beruht,** **(2) die zugehörigen Attribut-Zertifikate,** **(3) der der Signatur zuzuordnende Signaturschlüssel-Inhaber,**

[354] [assignment: *list of objects or information types*]

[355] [assignment: *list of subjects*]

(4) die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,

(5) das Ergebnis der Korrektheitsprüfung der Signatur,

(6) die Daten, auf die sich die Signatur bezieht,

(7) ob die signierten Daten unverändert sind,

(8) die Anforderung von OCSP-Anfragen und die Auswertung von OCSP-Antworten,

(9) die Anforderung von CRL-Anfragen und die Auswertung von CRL,

(10) [*none*][356].

Anwendungshinweis 167: Die Informationen aus dem OCSP-Dienst können eine gewisse Zeit in einem Cache gepuffert und verwendet werden. Dabei ist zu beachten, dass der verwendete Zeitpunkt der aus dem Cache entnommenen Prüfergebnisse nicht älter ist als der zu prüfende Signaturerstellungszeitpunkt. Der maximale Zeitraum der Verwendung des OCSP Cache kann vom Administrator vorgegeben werden.

Anwendungshinweis 168: Für die Prüfung der Zertifikate, der OCSP-Antworten und der OCSP-Zertifikate werden alle Verahren entsprechend Anwendungshinweis 161 und Anwendungshinweis 166 unterstützt.

FDP_ITC.2/AK.Sig	**Import of user data with security attributes / Signaturdienst**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/**AK.**Sig	The TSF shall enforce the *Signaturerstellung-SFP und Signaturprüfung-SFP*[357] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/**AK.**Sig	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/**AK.**Sig	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/**AK.**Sig	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

[356] **[assignment: *andere Form von Nachweisen*]**

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

FDP_ITC.2.5/**AK.**Sig The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) Die TSF importiert zu signierende Daten mit dem Sicherheitsattribut „Signaturrichtlinie“ nur nach erfolgreicher Prüfung der Zulässigkeit der Signaturrichtlinie.

(2) Die TSF importiert zu prüfende signierte Daten mit dem Sicherheitsattribut „Signaturrichtlinie“ nur nach erfolgreicher Prüfung der Zulässigkeit der Signaturrichtlinie.

(3) Eine Signaturrichtlinie für qualifizierte elektronische Signaturen ist zulässig, wenn

(a) für die Erzeugung einer qualifizierten elektronischen Signatur eine Benutzersteuerung festgelegt ist,

(b) die Signaturprüfung mit anzeigbarem erzeugtem Prüfprotokoll erfolgt,

(c) die Signaturrichtlinie auf die zu signierenden Daten durch den EVG anwendbar ist.

(4) Die TSF weist importierten zu signierenden Daten das Sicherheitsattribut „nicht autorisiert“ zu

.[358]

FMT_MSA.3/AK.Sig	**Static attribute initialisation / Signatur**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/**AK.**Sig	The TSF shall enforce the *Signaturerstellung-SFP und die Signaturprüfung-SFP*[359] to provide restrictive[360] default values for security attributes **zulässige Signaturrichtlinie** that are used to enforce the SFP.
FMT_MSA.3.2/**AK.**Sig	The TSF shall allow the *Administrator*[361] to specify alternative initial values to override the default values when an object or information is created.

Anwendungshinweis 169: Es sei darauf hingewiesen, dass Signaturrichtlinien in diesem Dokument weiter gefasst sind, s. Abschnitt 1.3.5.2. Diese und ggf. weitere Signaturpolicies können im EVG dauerhaft gespeichert sein.

FDP_SDI.2/AK	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring

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

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

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

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

Dependencies:	No dependencies.
FDP_SDI.2.1/AK	The TSF shall monitor ~~**user data**~~ **zu signierende Daten** stored in containers controlled by the TSF for *Veränderung*[362] on all objects, based on the following attributes: [*Signatur über die zu signierenden Daten*].
FDP_SDI.2.2/AK	Upon detection of a data integrity error, the TSF shall *(1) Die Erstellung der digitalen Signatur für die zu signierenden Daten verweigern und den Benutzer des Clientsystems über den Datenintegritätsfehler informieren,* *(2) [Nachdem die von der Chipkarte erzeugte Signatur über die zu signierenden Daten zurück an den Konnektor gesendet wurde, muss diese vom Konnektor erneut auf mathematische Korrektheit geprüft werden, bevor das Ergebnis an das Clientsystem ausgegeben werden darf.]* [363].

Anwendungshinweis 170: Die Verfeinerung des Elements FDP_SDI.2/**AK**.1 durch ersetzen von „Benutzerdaten“ durch „zu signierenden Daten“ präzisiert den besonderen Schutz dieser Daten. Die Zuweisung im Element FDP_SDI.2/**AK** wurde so gewählt, dass Veränderungen an den zu signierenden Daten ab der Übergabe durch den EVG bei Aufruf des Signierdienstes bis zur Rückgabe der signierten Daten an den EVG festgestellt werden können.

FMT_MSA.1/AK.User	**Management of security attributes / Clientsystem-Benutzer**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.
FMT_MSA.1.1/**AK.** User	The TSF shall enforce the *Signaturerstellung-SFP und die Signaturprüfung-SFP*[364] to restrict the ability to (1) Modify[365] the security attribute *Autorisierungsstatus zu signierender Daten,* [366]

[362] [assignment: *integrity errors*]

[363] [assignment: *action to be taken*]

[364] [assignment: *access control SFP(s), information flow control SFP(s)*]

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

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

(2) Select[367] **the security attribute gültige Signaturrichtlinie für zu signierende Daten,** [368]

(3) Modify[369] **the security attributes angegebener Zeitpunkt signierter Daten für die Signaturprüfung**[370]

to *S_Benutzer_Clientsystem*[371].

Anwendungshinweis 171: Die Operationen wurden zusammen mit den Sicherheitsattributen aufgelistet, um eine kompaktere Darstellung zu erreichen. Für den Autorisierungsstatus zu signierender Daten gilt die Regel (1) in FMT_MSA.1/AK.**User** in Verbindung mit den Regeln (1) und (2) in FMT_MSA.4/**AK**.1.

Die Auswahl der Signaturrichtlinie entsprechend Regel (2) sowie die Modifikation des angegebenen Zeitpunkts für die Signaturprüfung entsprechend Regel (3) erfolgt durch den S_Benutzer_Clientsystem über die Parametrisierung des Aufrufes der Entsprechenden Operationen der Signaturschnittstelle des EVG

FTP_ITC.1/**AK.**QSEE	Inter-TSF trusted channel / QSEE
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK.**QSEE	The TSF shall provide a communication channel between itself and ~~**another trusted IT product**~~ **der qualifizierten Signaturerstellungseinheit** 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** ~~**or**~~ disclosure.
FTP_ITC.1.2/**AK.**QSEE	The TSF shall permit the TSF[372] to initiate communication via the trusted channel.
FTP_ITC.1.3/**AK.**QSEE	The TSF shall initiate communication via the trusted channel for *Senden der zu signierende Daten an die qualifizierte Signaturerstellungseinheit*[373].

Anwendungshinweis 172: Die Verfeinerung des Elementes FTP_ITC.1/AK**.**QSEE konkretisiert den Signaturablauf. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „der qualifizierten Signaturerstellungseinheit“ verfeinert.

FTA_TAB.1/AK.Jobnummer Default TOE access banners / Jobnummer

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

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

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

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

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

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

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1.1/**AK.**Jobnummer	Before **entfernter Eingabe von PIN und PUK an eHealth-Kartenterminals ~~establishing a user session~~**, the TSF shall display **die vom Clientsystem übergebene und vom EVG geprüfte Jobnummer an eHealth-Kartenterminal ~~an advisory warning message~~** regarding **nichtbeabsichtigten ~~unauthorised~~** use of the TOE.

Anwendungshinweis 173: Die Verfeinerungen des Elements FTA_TAB.1/AK**.Jobnummer** präzisieren die Nutzung der Jobnummer. Die Benutzersitzung dieses Elements bezieht sich nur auf die „Eingabe von PIN oder PUK an den eHealth-Kartenterminals“ unter Steuerung des EVG und ist Teil einer Sitzung am Arbeitsplatz zur Signaturerstellung oder Entschlüsselung. Die Anzeige der „Jobnummern“ ist notwendig, um die korrekte Zuordnung zwischen der Sitzung am Clientsystems des Arbeitsplatzes und dem durch den EVG ausgewählten eHealth-Kartenterminal für die entfernte PIN-Eingabe zu ermöglichen.

FTA_TAB.1/AK.SP	**Default TOE access banners / Fehler des Signaturprozesses**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1.1/**AK.**SP	**~~Before establishing a user session~~ Bei Feststellung ungültig erzeugter Signaturen,** the TSF shall display an advisorywarning message regarding unauthorised use of the TOE **to S_Benutzer_Clientsystem via the standard interface**.

Anwendungshinweis 174: Die Verfeinerung des Elements FTA_TAB.1/AK**.SP** warnt den Benutzer bei festgestellten Fehlern des Signaturprozesses, wenn ungültig signierte Dateien festgestellt wurden über die Standard-Schnittstelle des Clientsystems. Die Bedingungen für ungültig signierte Dateien sind in FMT_MSA.4/**AK** festgelegt

6.3.3.5. Software-Update

FDP_ACC.1/AK.Update	**Subset access control / Update**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**Update	The TSF shall enforce the *Update-SFP*[374] on *subjects:* *(1) S_Administrator,* *(2) S_AK,* *(3) S_NK;* *objects:*

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

(1) Update-Pakete;
operations:
(1) Importieren
(2) Verwenden
' [375]

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

Tabelle 22: Operationen für Software-Update

FDP_ACF.1/AK.Update	**Security attribute based access control / Update**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**Update	The TSF shall enforce the *Update-SFP* [376] to objects based on the following: *subjects:* *(1) S_Administrator* *(2) S_AK,* *(3) S_NK* *objects:* *(1) Update-Pakete with security attributes:* *a. Signatur,* *b. Zulässige Software-Versionen* .

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

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

FDP_ACF.1.2/**AK.**Update	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Das Subjekt S_AK oder S_NK darf nur Update-Pakete importieren, deren Signatur erfolgreich geprüft wurde.* *(2) Die Subjekte S_Administrator, S_AK und S_NK dürfen nur Update-Pakete verwenden, die einer Firmwaregruppe angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist.* .[377]
FDP_ACF.1.3/**AK.**Update	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][378].
FDP_ACF.1.4/**AK.**Update	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. *S_AK und S_NK dürfen Update-Pakete nicht automatisch anwenden, wenn die automatische Aktualisierung der Firmware durch S_Administrator deaktiviert wurde.* 2. *Wenn MGM_LU_ONLINE=Disabled gesetzt ist, so darf die TSF keine Kommunikation mit dem Update-Server (KSR) herstellen.* .[379].

Anwendungshinweis 175: Die Liste der zulässigen Software-Versionen wird in der Spezifikation *Übergreifende Spezifikation: Operations und Maintenance* [gemSpec_OM] mit "Firmware-Gruppe" bezeichnet [43]. Diese ist als versionierte Liste zulässiger Firmware-Versionen für Software-Updates in jede Konnektor-Software integriert werden.

FDP_UIT.1/AK.Update	**Data exchange integrity / Update**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

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

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

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

FDP_UIT.1.1/**AK.**Update	The TSF shall enforce the *Update-SFP*[380] to receive[381] user data ~~**in a manner**~~ protected from modification, deletion, insertion errors.[382].
FDP_UIT.1.2/**AK.**Update	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion[383] has occurred.

6.3.3.6. Verschlüsselungsdienst

FDP_ACC.1/AK.Enc	**Subset access control / Verschlüsselung**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**Enc	The TSF shall enforce the *Verschlüsselung-SFP*[384] on *subjects:* *(1) S_AK,* *(2) S_Verschlüsselungsdienst;* *objects:* *(1) Zu verschlüsselnde Daten,* *(2) Verschlüsselte Daten,* *(3) Zu entschlüsselnde Daten,* *(4) Entschlüsselte Daten;* *operations:* *(1) Verschlüsseln,* *(2) Entschlüsseln,* *(3) Festlegen der vorgesehenen Empfänger*[385]

Operation	Beschreibung	Anmerkung
Verschlüsseln	Hybridverschlüsselung von XML-Dokumenten gemäß FCS_COP.1/AK.XML.Ver und beliebige Datendateien nach FCS_COP.1/AK.CMS.Ver oder symmetrische Verschlüsselung von Daten gemäß FCS_COP.1/AK.AES	
Entschlüsseln	Hybridentschlüsselung von XML-Dokumenten mit Unterstützung der Chipkarte für die asymmetrische	

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

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

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

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

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

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

	Entschlüsselung gemäß FCS_COP.1/AK.XML.Ent und beliebige CMS-Datendateien nach FCS_COP.1/AK.CMS.Ent oder symmetrische Entschlüsselung von Daten gemäß FCS_COP.1/AK.AES	
Festlegen der vorgesehenen Empfänger	Durch S_AK werden die zu verschlüsselnde Daten an das Subjekt S_Verschlüsselungsdienst mit der Identität der vorgeschlagenen Empfängern übergeben.	

Tabelle 23: Operationen des Verschlüsselungsdienstes

FDP_ACF.1/AK.Enc	**Security attribute based access control / Verschlüsselung**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**Enc	The TSF shall enforce the *Verschlüsselung-SFP* [386] to objects based on the following: *subjects:* *(1) S_AK,* *(2) S_Verschlüsselungsdienst;* *objects:* (1) *Zu verschlüsselnde Daten with security attributes:* *(a) Verschlüsselungsrichtlinie,* *(b) Vorgeschlagene Empfänger,* *(c) Objekt-ID,* (2) *verschlüsselte Daten with security attributes:* *(a) Verschlüsselungsrichtlinie,* *(b) Vorgeschlagene Empfänger,* *(c) Ordnungsgemäss verschlüsselt,* (3) *Zu entschlüsselnde Daten with security attributes:* *(a) Verschlüsselungsrichtlinie,* *(b) Vorgeschlagene Empfänger* (4) *Entschlüsselte Daten* . [387]
FDP_ACF.1.2/**AK.**Enc	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

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

[387] [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*]

(1) Das Subjekt S_AK muss zu verschlüsselnde Daten an das Subjekt Verschlüsselungsdienst mit der Objekt-ID, der Identität der Verschlüsselungsrichtlinie und der Identität der vorgeschlagenen Empfängern übergeben.

(2) Das Subjekt Verschlüsselungsdienst darf nur ordnungsgemäß verschlüsselte Daten oder Statusmeldungen an das Subjekt S_AK zurückgeben.

(3) Das Subjekt Verschlüsselungsdienst darf nur dann die zu verschlüsselnden Daten für die identifizierten vorgeschlagenen Empfänger automatisch verschlüsseln, wenn

(a) die identifizierte Verschlüsselungsrichtlinie für die übergebenen zu verschlüsselnden Daten zulässig ist,

(b) die identifizierte Verschlüsselungsrichtlinie die automatische Verschlüsselung erlaubt,

(c) die Verschlüsselungszertifikate der vorgeschlagenen Empfänger gültig sind.

(4) Das Subjekt S_AK darf zu entschlüsselnde Daten an das Subjekt Verschlüsselungsdienst nur mit Identität eines vorgesehenen Empfängers, dessen Chipkarte für die Entschlüsselung benutzt werden soll, und der Identität der zum Entschlüsseln zu verwendenden Verschlüsselungsrichtlinie an das Subjekt Verschlüsselungsdienst übergeben.

(5) Das Subjekt Verschlüsselungsdienst darf nur dann die verschlüsselten Daten automatisch für die identifizierten vorgesehenen Empfänger entschlüsseln und die entschlüsselten Daten an die Subjekt S_AK zurückgeben, wenn

(a) die identifizierte Verschlüsselungsrichtlinie für die übergebenen zu verschlüsselten Daten zulässig ist,

(b) die identifizierte Verschlüsselungsrichtlinie die automatische Entschlüsselung erlaubt,

(c) der Sicherheitsstatus der Chipkarte des identifizierten vorgesehenen Empfängers das Entschlüsseln des Dateischlüssels erlaubt.

.[388]

FDP_ACF.1.3/**AK.**Enc The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][389].

FDP_ACF.1.4/**AK.**Enc The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*][390].

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

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

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

Anwendungshinweis 176: Alle Verschlüsselungsrichtlinie für Konnektoren erlauben das automatische Verschlüsseln und Entschlüsseln von Daten. Die zum Entschlüsseln zu verwendende Chipkarte hängt von dem identifizierten vorgesehenen Empfänger und der auszuführenden Anwenungen ab.

FDP_ITC.2/AK.Enc	**Import of user data with security attributes / Verschlüsselungsdienst**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/**AK.**Enc	The TSF shall enforce the *Verschüsselungs-SFP*[391] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/**AK.**Enc	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/**AK.**Enc	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/**AK.**Enc	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/**AK.**Enc	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *(1) Die TSF importiert zu verschlüsselnde Daten mit dem Sicherheitsattribut „Verschlüsselungsrichtlinie“ nur für die identifizierten Fachanwendungen bzw. Anwendungsfälle und implementierten Verschlüsselungsrichtlinien.* *(2) Die TSF importiert Verschlüsselungszertifikate und zu verschlüsselnde Daten mit dem Sicherheitsattribut „vorgeschlagene Empfänger“ nur nach erfolgreicher Prüfung der Gültigkeit der Verschlüsselungszertifikate der vorgesehenen Empfänger.* *(3) Die TSF importiert TI-fremde X.509 CA-Zertifikate durch den Administrator über die Management-Schnittstelle* .[392]

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

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

Anwendungshinweis 177: Die Verschlüsselungsrichtlinie ist eindeutig durch die Fachanwendung bzw. innerhalb der Fachanwendung durch den Anwendungsfalls festgelegt und muss dem Verschlüsselungs- dienst für die übergebenen Daten angezeigt werden. Ein Verschlüsselungszertifikat ist gültig, wenn

- Entweder (i) seine Integrität durch eine Zertifikatskette bis zu einer Instanz aus der TSL mit als authentisch bekannten öffentlichen Schlüssel erfolgreich geprüft wurde und (ii) das Verschlüsselungszertifikat nicht gesperrt ist (Prüfung mittels OCSP-Abfrage),
- oder seine Integrität durch eine Zertifikatskette bis zu einer Instanz aus der Liste der TI-fremden CA-Zertifikate für die hybride Verschlüsselung (CERT_IMPORTED_CA_LIST) mit als authentisch bekannten öffentlichen Schlüssel erfolgreich geprüft wurde.

FDP_ETC.2/AK.Enc	**Export of user data with security attributes / Verschlüsselungsdienst**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/**AK.**Enc	The TSF shall enforce the *Verschüsselungs-SFP*[393] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2/**AK.**Enc	The TSF shall export the user data with the user data's associated security attributes
FDP_ETC.2.3/**AK.**Enc	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/**AK.**Enc	The TSF shall enforce the following rules when user data is exported from the TOE: *(1) Die TSF exportieren verschlüsselte Daten mit der Identität des vorgesehenen Empfängers bzw. den Identitäten der vorgesehenen Empfänger und der Identität der verwendeten Verschlüsselungsrichtlinie.* *(2) Die TSF exportieren entschlüsselte Daten mit der Identität des vorgesehenen Empfängers, dessen Chipkarte zum Entschlüsseln benutzt wurde.* *(3) [none]* [394]*.* *.* [395]

6.3.3.7. TLS-Kanäle

Dieses Kapitel beschreibt die Anforderungen, die an die TLS-Kanäle des EVG gestellt werden, die durch den TLS-Dienst für die Kommunikationsverbindungen:

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

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

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

- Von Fachmodulen zu den Fachdiensten
- Von Clientsystemen mit dem EVG Konnektor
- EVG zum Verzeichnisdienst
- EVG zum Konfigurationsdienst
- EVG zum TSL-Dienst für den Download der BNetzA-VL und deren Hash-Wert

genutzt werden.

Gemäß TIP1-A_7254 in [27] muss der EVG bei einem Aufbau von TLS-gesicherten Verbindungen zu einem zentralen Dienst der TI-Plattform oder zu einem fachanwendungsspezifischen Dienst bei folgenden OCSP-Antworten, die der EVG entsprechend FTP_ITC.1/NK.TLS ermittelt, mit einem Abbruch des Verbindungsaufbaus reagieren:

•CERT_REVOKED;

•CERT_UNKNOWN;

•OCSP_CHECK_REVOCATION_FAILED.

Die Behandlung anderer etwaiger Fehlerfälle bei einem TLS-Verbindungsaufbau bleiben dadurch unberührt. Die genannte Verschärfung wurde in diesen Sicherheitsvorgaben dadurch berücksichtigt, dass in FDP_ACF.1/AK.TLS, Fußnote 266, eine explizit verbietende Regel für die Zuweisung, die BSI CC PP 0098 vorsieht, eingesetzt wurde.

FDP_ACC.1/AK.TLS	**Subset access control / TLS-Kanäle**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**TLS	The TSF shall enforce the *AK-TLS-SFP*[396] on *subjects:* *(1) S_AK,* *(2) S_NK* *(3) S_Clientsystem,* *(4) S_Fachmodul,* *(5) S_ Fachdienst,* *(6) S_Verzeichnisdienst (VZD),* *(7) S_KSR* *(8) S_TSL_Dienst* *(9) S_Administrator* *objects:* *(1) Zu sendende Daten,*

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

(2) Empfangene Daten,

(3) TLS-Kanal

operations:

(1) Aufbau des TLS-Kanals,

(2) Abbau des TLS-Kanals

(3) Unterbrechen und Wiederaufnahme der TLS-Verbindung mit Session ID (nur VSDM),

(4) Anfordern zur Wiederaufnahme einer TLS- Verbindung mit Session ID (nur VSDM),

(5) senden

(6) empfangen

[397].

Operation	Beschreibung	Anmerkung
Aufbau des TLS-Kanals	Vor Beginn der geschützten Datenübertragung wird ein TLS-Kanal zum Kommunikationspartner aufgebaut: (1) Bei der Kommunikation des EVG mit S_Verzeichnisdienst (VZD), S_KSR oder S_TSL_Dienst wird eine einseitige (Server) Authentifizierung (Identität C.ZD.TLS-S) durch den EVG durchgeführt. (2) Bei der Kommunikation des EVG mit S_ Fachdienst findet je nach Aufruf durch S_ Fachdienst eine einseitige (Server) oder beidseitige Authentisierung statt. Der EVG nutzt bei der beidseitigen Authentisierung die C.HCI.AUT Identität des X.509 Zertifikats auf der SMC-B für die Client-Authentisierung. S_ Fachdienst nutzt stets das X.509 Zertifikat C.FD.TLS-S für die Server-Authentisierung.	Algorithmen und Schlüssel für die Kanalverschlüsselung werden mit dem Kommunikationspartner ausgehandelt. Dem TLS-Kanal wird ein TLSConnectionIdentifier zugeordnet.

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

Operation	Beschreibung	Anmerkung
	(3) Bei der Kommunikation des EVG mit S_Clientsystem muss der Konnektor als TLS-Server die Authentifizierung des Clientsystems mit den Verfahren Basic Authentication (Username/ Password) [RFC2617] über http/TLS [RFC2818] und zertifikatsbasierte Client-Authentifizierung (X.509) [gemSpec_PKI#8.3.1.4] über TLS anbieten (vergl. [27], Kap. 3.4). Der EVG nutzt in diesem Fall das Schlüsselmaterial der Identität des X.509 Zertifikats C.AK.AUT der gSMC-K oder ein X.509 Zertifikats das entsprechend FCS_CKM.1/NK.Zert erzeugt bzw. entsprechend FDP_ITC.2/NK.TLS importiert wurde (ID.AK.AUT). (4) Bei der Kommunikation des EVG mit gepaarten Kartenterminals findet eine beidseitige Authentisierung statt. Das Kartenterminal nutzt hier das Schlüsselmaterial des C.SMKT_AUT Zertifikates. Der EVG verwendet das Schlüsselmaterial der Identität ID.SAK.AUT.	
Abbau des TLS-Kanals	Nach Ende der Kommunikation wird der TLS-Kanal abgebaut.	Die Schlüssel werden sicher gelöscht und die Ressourcen werden freigegeben.
Unterbrechen und Wiederaufnahme der TLS-Verbindung mit Session ID (nur VSDM)	Unterbrechen und Wiederaufnahme einer TLS-Verbindung zwischen S_Fachmodul (VSDM) und Intermediär durch TLS Session Resumption mittels Session-ID gemäß RFC 5246.	TLS Session Resumption ist nur zulässig, wenn das Schlüsselmaterial nicht älter als 24 Stunden ist.
Anfordern zur Wiederaufnahme	Das S_Fachmodul (VSDM) fordert die Wiederaufnahme der Sitzung des	Der Intermediär VSDM kann die Wiederaufnahme der Sitzung

Operation	Beschreibung	Anmerkung
einer TLS-Verbindung (nur VSDM)	Kanals unter Verwendung des Session-ID gemäß RFC 5246, Kap. 7.3, beim Intermediär VSDM an.	des Kanals mit Session-ID akzeptieren oder ablehnen.
Senden	Die zu übertragenden Daten werden vor Übertragung verschlüsselt und integritätsgeschützt	Die beim Kanal-Aufbau ausgehandelten Algorithmen und Sitzungs-Schlüssel werden verwendet.
Empfangen	Die empfangenen Daten werden entschlüsselt und integritätsgeprüft. Es werden unverfälscht empfangene Daten ausgegeben.	Die beim Kanal-Aufbau ausgehandelten Algorithmen und Sitzungs-Schlüssel werden verwendet.

Tabelle 24: Operationen der TLS-Kanäle

FDP_ACF.1/AK.TLS	**Security attribute based access control / TLS-Kanäle**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**TLS	The TSF shall enforce the *AK-TLS-SFP*[398] to objects based on the following: *subjects:* (1) *S_AK,* (2) *S_NK* (3) *S_Clientsystem,* (4) *S_Fachmodul with or without the security attribute "VSDM (VSDM-Fachmodul)",* (5) *S_ Fachdienst with or without the security attribute "Intermediär VSDM (Intermediär VSDM)",* (6) *S_Verzeichnisdienst (VZD),* (7) *S_KSR* (8) *S_TSL_Dienst* *objects:* (1) *Zu sendende Daten,* (2) *Empfangene Daten,*

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

(3) *TLS-Kanal with the security attribute „Anfordernder TLS-Client“*

.[399]

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

(1) Das S_AK baut auf Anforderung des Fachmoduls die TLS-Verbindung zum Fachdienst (TLS Server) auf und gibt den TLSConnectionIdentifier an den Aufrufenden zurück.

(2) Auf Anforderung des Clientsystems (als TLS Client) baut das S_AK (als TLS-Server) ein TLS-Kanal zum Clientsystem auf.

(3) Nur der anfordernde TLS-Client darf unter Angabe des TLSConnectionIdentifiers zu sendende Daten an das S_AK zur Übertragung im TLS-Kanal übergeben.

(4) Das S_AK darf über den TLS-Kanal empfangene Daten nur an den anfordernden TLS-Client übergeben.

(5) Nur der anfordernde TLS-Client darf den S-AK zum Abbau des TLS-Kanals auffordern.

(6) Wenn MGM_LU_ONLINE=Enabled darf das S_AK ein SessionID des Intermediär VSDM empfangen und dem TLSConnectionIdentifier zuordnen. Das S_AK darf auf Anforderung des VSDM-Fachmoduls die unterbrochene Sitzung des TLS-Kanals zum Intermediär VSDM mit dem SessionID wiederaufnehmen, wenn das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial nicht älter als 24 Stunden ist.

(7) Wenn MGM_LU_ONLINE=Enabled und MGM_LOGICAL_SEPARATION=Disabled dann baut das S_AK mit dem LDAP-Proxy auf Anforderung des Clientsystems oder eines Fachmoduls (Search Request) eine LDAPv3 Verbindung zum VZD auf.

(8) Wenn MGM_LU_ONLINE=Enabled und MGM_LOGICAL_SEPARATION=Disabled dann baut das S_AK mit dem LDAP-Proxy auf Anforderung des Clientsystems oder eines Fachmoduls (Unbind Request) eine LDAPv3 Verbindung zum VZD ab.

(9) Wenn ANCL_TLS_MANDATORY = Enabled so nimmt S_AK die Aufforderung des Clientsystems zum Aufbau eines TLS-Kanals entgegen und darf nur über diesen Kanal mit Clientsystemen

[399] [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*]

kommunizieren. Ausgenommen ist die Kommunikation mit Dienstverzeichnisdienst bei gesetzter Variable ANCL_DVD_OPEN = Enabled.

(10) Die Subjekte S_NK und S_AK dürfen für den Download von Firmware-Update-Paketen einen TLS-Kanal zum S_KSR aufbauen.

(11) Das S_AK baut für den Download der BNetzA-VL und deren Hash-Wert und TSL-Hash-Werte einen TLS-Kanal zum TSL-Dienst auf.

(12) [none][400].

[401].

FDP_ACF.1.3/**AK.**TLS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][402].

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

(1) Wenn MGM_LU_ONLINE = "Disabled", DARF der Basisdienst TLS-Dienst nach dem Bootup NICHT TLS-Kanäle zur Verfügung stellen.

(2) Der Intermediär VSDM kann die Nutzung der SessionID zur Wiederaufnahme der TLS-Verbindung ablehnen und den Aufbau einer TLS-Verbindung verlangen.

(3) Wenn MGM_LU_ONLINE = "Disabled" oder MGM_LOGICAL_SEPARATION=Enabled, DARF die Verzeichnisverwaltung NICHT TLS-Kanäle zum VZD zur Verfügung stellen.

(4) The TSF shall perform den Kanal zum VZD 15 Minuten nach der letzten vom VZD empfangenen oder von der Verzeichnisverwaltung des EVG gesendeten Daten abbauen.

(5) [Falls bei einer Verbindung zu einem der Subjekte S_ Fachdienst, S_TSL_Dienst, S_KSR, S_VSDD_Fachdienst oder S_Verzeichnisdienst (VZD) die OCSP-Antwort

- *CERT_REVOKED, oder*
- *CERT_UNKNOWN, oder*
- *OCSP_CHECK_REVOCATION_FAILED*

lautet, so muss der EVG den Verbindungsaufbau abbrechen] [403]

---

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

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

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

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

[404].

Anwendungshinweis 178: [30] bestimmt in GS-A_5322, dass der EVG im Rahmen von TLS-Session-Resumption mittels SessionID (vgl. [RFC-5246, Abschnitt 7.4.1.2]) nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) sowie damit verbundene SessionIDs sicher gelöscht werden. Das Fachmodul VSDM und der Intermediär VSDM müssen für die Verbindung zwischen Fachmodul und Intermediär TLS Session Resumption mittels Session-ID gemäß RFC 5246 nutzen, um für den wiederholten Aufbau von TLS-Verbindungen die bereits ausgehandelten Session-Parameter zu nutzen.

Anwendungshinweis 179: Der Konnektor muss beim TLS-Verbindungsaufbau den OCSP-Status des TLS-Serverzertifikates gemäß TIP1-A_7254 [27] beachten.

FMT_MSA.1/AK.TLS	**Management of security attributes / TLS-Kanäle**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.
FMT_MSA.1.1/**AK.**TLS	The TSF shall enforce the *AK-TLS-SFP*[405] to restrict the ability to change_default, query, modify, delete, [*no other operations*][406] the security attributes [***Authentisierungsmechanismus***][407] to *S_Administrator*[408]. **Änderungen der Konfiguration müssen unmittelbar durchgesetzt werden.**

Anwendungshinweis 180: Die in FMT_MSA.1/AK.**TLS** definierte Verfeinerung bezieht sich insbesondere auf solche Konfigurationen, die die Art der akzeptierten Authentisierungsmechanismen betreffen, etwa ANCL_CAUT_MODE [27].

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

[405] [assignment: *access control SFP(s), information flow control SFP(s)*]

[406] [assignment: other operations], (die Auswahl wurde im PP vorgenommen, alle 4 vordefinierten Werte wurden ausgewählt, außerdem wurde die Möglichkeit, andere Optionen zuzuweisen, ebenfalls zugelassen)

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

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

FMT_MSA.3/AK.TLS	**Static attribute initialisation / TLS-Kanäle**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/**AK.**TLS	The TSF shall enforce the *AK-TLS-SFP*[409] to provide [restrictive][410] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/**AK.**TLS	The TSF shall allow the *S_Administrator*[411] to specify alternative initial values to override the default values when an object or information is created.

FTP_ITC.1/AK.FD	**Inter-TSF trusted channel / Zum Fachdienst**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK.**FD	The TSF shall provide a communication channel between itself and **a S_ Fachdienst** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_ Fachdienst mit dem Zertifikat C.FD.TLS-S gegenüber dem EVG und EVG mit dem Zertifikat C.HCI.AUT gegenüber S_Fachdienst wenn von S_Fachmodul gefordert** ~~its end points~~ and protection of the channel data from modification **and** ~~**or**~~ disclosure.
FTP_ITC.1.2/**AK.**FD	The TSF shall permit the TSF[412] to initiate communication via the trusted channel
FTP_ITC.1.3/**AK.**FD	The TSF shall initiate communication via the trusted channel for *die Bearbeitung von fachlichen Anwendungsfällen, die eine Online-Kommunikation mit Fachdiensten erfordern*[413]

Anwendungshinweis 181: Die Verfeinerung des Elementes FTP_ITC.1/AK.FD konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „Fachdienst“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem Fachdienst auf, wobei die Authentisierung der Endpunkte je nach Aufruf durch das Fachmodul beidseitig ist oder auf den Fachdienst eingeschränkt wird.

FTP_ITC.1/AK.VZD Inter-TSF trusted channel / Zum zentralen Verzeichnisdienst

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

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

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

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

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK.**VZD	The TSF shall provide a communication channel between itself and **S_Verzeichnisdienst (**VZD) ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_Verzeichnisdienst (**VZD) **mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and ~~or~~** disclosure.
FTP_ITC.1.2/**AK.**VZD	The TSF shall permit the TSF[414] to initiate communication via the trusted channel.
FTP_ITC.1.3/**AK.**VZD	The TSF shall initiate communication via the trusted channel for *MGM_LU_ONLINE=Enabled und MGM_LOGICAL_SEPARATION=Disabled des TUC_KON_290 „LDAP-Verbindung aufbauen“*[415].

Anwendungshinweis 182: Die Verfeinerung des Elementes FTP_ITC.1/VZD konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „zentralen Verzeichnisdienst“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem zentralen Verzeichnisdienst (VZD) auf, wobei die Authentisierung der Endpunkte auf den VZD eingeschränkt wird. Gemäß OE.Fachdienste können nur verrauenswprdige Entitäten auf den VZD zugreifen.

FTP_ITC.1/AK.KSR	**Inter-TSF trusted channel / Zum KSR (Update-Server)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK**.KSR	The TSF shall provide a communication channel between itself and **S_KSR** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_KSR mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and ~~or~~** disclosure..
FTP_ITC.1.2/**AK**.KSR	The TSF shall permit the TSF[416] to initiate communication via the trusted channel.
FTP_ITC.1.3/**AK.**KSR	The TSF shall initiate communication via the trusted channel for *Prüfung auf neue Firmware-Update-Pakete und Download neuer Firmware-Update-Pakete*[417].

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

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

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

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

Anwendungshinweis 183: Die Verfeinerung des Elementes FTP_ITC.1/KSR konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „KSR“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem KSR (Update-Server) auf, wobei die Authentisierung der Endpunkte auf den KSR eingeschränkt wird.

FTP_ITC.1/AK.TSL	**Inter-TSF trusted channel / Zum TSL-Dienst**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK**.TSL	The TSF shall provide a communication channel between itself and **S_TSL_Dienst** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_TSL_Dienst mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and** ~~**or**~~ disclosure..
FTP_ITC.1.2/**AK**.TSL	The TSF shall permit the TSF[418] to initiate communication via the trusted channel.
FTP_ITC.1.3/**AK.**TSL	The TSF shall initiate communication via the trusted channel for *Download des TSL-Hashwertes, BNetzA-VL Hashwerts und Download der BNetzA-VL*[419].

Anwendungshinweis 184: Die Verfeinerung des Elementes FTP_ITC.1/TSL konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „TSL-Dienst“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem TSL-Dienst auf, wobei die Authentisierung der Endpunkte auf den TSL-Dienst eingeschränkt wird.

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

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

FTP_ITC.1/AK.CS	**Inter-TSF trusted channel / Clientsystem**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK.**CS	The TSF shall provide a communication channel between itself and **a Clientsystem in the LAN ~~another 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 ~~or~~** disclosure.
FTP_ITC.1.2/**AK.**CS	The TSF shall permit **the Clientsystem**[420] to initiate communication via the trusted channel.
FTP_ITC.1.3/**AK.**CS	The TSF shall initiate communication via the trusted channel for *ANCL_TLS_MANDATORY = Enabled*[421] **to the Clientsystem and reject or cancel a communication with the Clientsystem outside the TLS channel. This includes access to the service directory service.** **A communication with the service directory service outside the TLS channel is only permitted if ANCL_DVD_OPEN is set to "Enabled".**

Anwendungshinweis 185: Die Verfeinerung des Elementes FTP_ITC.1/AK**.CS** konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt" wurde durch „Clientsystem im LAN" verfeinert. Die Verfeinerung im Element FTP_ITC.1.3/CS soll klar stellen, dass in der speziellen Konfiguration der TSF ANCL_TLS_MANDATORY = Enabled die TLS-Kommunikation mit Ausnahme des Dienstverzeichnisdienstes erzwungen wird, während sie für ANCL_TLS_MANDATORY = Disabled auch Kommunikation außerhalb TLS erlaubt ist. Der Dienstverzeichnisdienst ist innerhalb des TLS-Kanals und im Fall ANCL_DVD_OPEN = Enabled auch außerhalb des TLS-Kanals erreichbar (s. [27], Kapitel 3.4.1). Da der TLS-Kanal einen Schutz des EVG gegen Missbrauch bietet, sollte die ungeschützte offene Kommunikation auf den Dienstverzeichnisdienst begrenzt werden.

FTP_ITC.1/AK.eHKT	**Inter-TSF trusted channel / eHKT**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/**AK.**eHKT	The TSF shall provide a communication channel between itself and another **eHealth-Kartenterminal ~~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 ~~or~~** disclosure. **Die TSF muss einen Keep-Alive-Mechanismus der TLS-Verbindung zu den eHealth-Kartenterminals implementieren.**

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

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

FTP_ITC.1.2/**AK.**eHKT	The TSF shall permit another trusted IT product[422] **eHealth-Kartenterminal** to initiate communication via the trusted channel
FTP_ITC.1.3/**AK.**eHKT	The TSF shall initiate communication via the trusted channel for *Senden von SICCT-Kommandos an eHealth-Kartenterminals und Empfangen von SICCT-Antworten der eHealth-Kartenterminals an den EVG*[423].

Anwendungshinweis 186: Die Verfeinerung des Elementes FTP_ITC.1/AK**.eHKT** konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „eHealth-Kartenterminal“ verfeinert.

6.3.3.8. Sicherer Datenspeicher

FDP_ACC.1/AK.SDS	**Subset access control / Sicherer Datenspeicher**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**SDS	The TSF shall enforce the *SDS-SFP*[424] on *subjects:* *(1) S_AK,* *(2) S_Fachmodul,* *(3) S_Administrator* *objects:* *(1) Schlüssel für sicheren Datenspeicher,* *(2) Datenobjekte des sicheren Datenspeichers,* *operations:* *(1) lesen* *(2) schreiben* .[425]

Operation	Beschreibung	Anmerkung
Lesen	Für den Zugriff auf den Inhalt des sicheren (geschützten) Datenspeichers durch den Konnektor ist die Nutzung des	Der sichere Datenspeicher muss während der gesamten Betriebszeit des Konnektors zur Verfügung

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

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

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

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

	Schlüsselmaterials erforderlich. Dazu muss dieser gelesen werden können.	stehen, so dass das Lesen des Schlüsselmaterials jeweils zu Beginn des Betriebes erfolgen soll.
Schreiben	Der Schreibzugriff auf das Schlüsselmaterial ist zur Erstellung und Änderung des Schlüssels erforderlich.	Die Erstellung der Schlüssel sollte einmalig durch den Administrator erfolgen. Optional kann ein Schlüsselwechsel durch den Administrator vorgesehen werden.

Tabelle 25: Operationen zum Zugriff auf die eGK im Rahmen von VSDM

FDP_ACF.1/AK.SDS	**Security attribute based access control / Sicherer Datenspeicher**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**SDS	The TSF shall enforce the *SDS-SFP*[426] to objects based on the following: *subjects:* (1) *S_AK,* *(3) S_Fachmodul,* *(4) S_Administrator* *objects:* *(1) Datenobjekte des sicheren Datenspeichers,* (2) *Datenobjekte des sicheren Datenspeichers with security attribute Administratorobjekt.*[427]
FDP_ACF.1.2/**AK.**SDS	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Das S_AK darf Datenobjekte im sicheren Datenspeicher nur verschlüsselt speichern.* *(2) Das S_AK darf nach Inbetriebnahme des Konnektors die Datenobjekte des SDS mit dem Sicherheitsattribut „allgemeines Datenobjekt“ lesen, entschlüsseln und außerhalb des sicheren Datenspeichers nur temporär speichern,*

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

[427] [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*]

(3) Das S_Fachmodul darf Daten an den S_AK übergeben und vom S_AK empfangen, die der S_AK als Datenobjekte des SDS mit dem Sicherheitsattribut „allgemeines Datenobjekt“ speichert,

(4) Datenobjekte des SDS mit dem Sicherherheitsattribut „Adminstratorobjekt“ darf nur innerhalb einer Administratorsitzung entschlüsselt und gelesen und verschlüsselt und geschrieben werden, aber nicht außerhalb der Administratorsitzung gespeichert werden,

(5) *[no additional rules]* [428].
[429]

FDP_ACF.1.3/**AK.**SDS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*] [430].

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

(1) Das S_AK darf Datenobjekte des SDS mit dem Sicherherheitsattribut „Adminstratorobjekt“ weder lesen noch entschlüsseln.

(2) Das S_AK darf keine Datenobjekte des SDS mit dem Sicherherheitsattribut „Adminstratorobjekt“ speichern oder modifizieren.

(3) *[no additional rules,]* [431].
[432]

Anwendungshinweis 187: Der sichere Datenspeicher ist in Form einer transparenten Speicherverschlüsselung (CFS) realisiert. Temporär gespeicherte Datenobjekte aus dem sicheren Datenspeicher sind im abgeschalteten Zustand des Konnektors nicht zugänglich. Für den Zugriff auf die dazu nötigen Schlüssel wird die gSMC-K (als Speicherort) verwendet.

Anwendungshinweis 188: Das CFS setzt eine transparente Speicherverschlüsselung um. Klartextdaten werden dabei in den temporären Speicher geladen (volatile memory). Bei ausgeschaltetem Konnektor ist der temporäre Speicher leer und die Inhalte des sicheren Datenspeichers liegen nur noch in vereschlüsselter Form im CFS. Das CFS wird im Rahmen des sicheren Bootvorgangs initialisiert. Der verschlüsselt im Konnektor abgelegte CFS-Schlüssel wird durch den in der gSMC-K sicher gespeicherten asymmetrischen Schlüssel entschlüsselt.

Anwendungshinweis 189: Datenobjekte des SDS mit dem Sicherherheitsattribut „Adminstratorobjekt“ werden vom Konnektor nicht unterstützt.

---

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

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

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

[431] [assignment: additional rules, based on security attributes, that explicitly deny access of subjects to objects].

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

6.3.3.9. Fachmodule

FDP_ACC.1/AK.VSDM	**Subset access control / VSDM**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/**AK.**VSDM	The TSF shall enforce the *VSDM-SFP*[433] on *subjects:* *(1) S_AK,* *(2) S_VSDM_Fachmodul,* *(3) S_VSDM_Intermediär,* *(4) S_VSDD_Fachdienst,* *(5) S_CMS,* *(6) S_eGK* *(7) S_Administrator;* *objecte:* *(1) Daten der Chipkarten (Versichertenstammdaten),* *(2) Objektsystem der Chipkarte (eGK);* *operations:* *(1) Lesen der Versichertenstammdaten,* *(2) Schreiben der Versichertenstammdaten,* (3) *Ergänzen des Objektsystems* .[434]

Operation	Beschreibung	Anmerkung
Lesen der Versichertenstammdaten	Lesen der Versicherten-stammdaten der eGK	Diese Operation kann die Kartenkommandos SELECT, SEARCH BINARY, READ BINARY, SEARCH RECORD, READ RECORD erfordern
Schreiben der Versichertenstammdaten	Schreiben oder Modifizieren der	Diese Operation kann die Kartenkommandos SELECT, ERASE BINARY, , UPDATE BINARY, WRITE BINARY,

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

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

	Versicherten-stammdaten der eGK	APPEND RECORD, ERASE RECORD, UPDATE RECORD, WRITE RECORD erfordern
Ergänzen des Objektsystems	Anlegen neuer Objekte des Objektsystems der eGK	Diese Operation erfordert die Kartenkommandos SELECT und LOAD APPLICATION.

Tabelle 26: Operationen zum Zugriff auf die eHK im Rahmen von VSDM

FDP_ACF.1/AK.VSDM	**Security attribute based access control / VSDM**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/**AK.**VSDM	The TSF shall enforce *VSDM-SFP*[435] to objects based on the following: *subjects:* *(1) S_AK,* *(2) S_VSDM_Fachmodul,* *(3) S_VSDM_Intermediär,* *(4) S_VSDD_Fachdienst,* *(5) S_CMS,* *(6) S_eGK;* *objects:* *(1) Daten der Chipkarten (Versichertenstammdaten) with the security attribute:* *a. „geschützt“* *b. „ungeschützt“* *(2) Objektsystem der Chipkarte (eGK)* .[436]
FDP_ACF.1.2/**AK.**VSDM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Der S_VSDM_Fachmodul kommuniziert mit dem VSDD und dem CMS über den VSDM_Intermediär und fordert dafür die*

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

[436] [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*]

Bereitstellung eines TLS-Kanals mit gegenseitiger Authentisierung gemäß FTP_ITC.1/AK.FD durch S_AK an.

(2) Bei Zugriff des VSDD_Fachdienst oder des CMS auf die eGK ermöglicht S_VSDM_Fachmodul den Aufbau eines Secure Messaging Kanals zwischen VSDD_Fachdienst bzw. CMS und der eGK.

(3) Zugriffe auf S_eGK durch S_VSDD_Fachdienst werden vom S_AK (Chipkartendienst) auf dem Objektsystem der eGK protokolliert.

(4) *[none]*[437]

.[438]

FDP_ACF.1.3/**AK.**VSDM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][439].
FDP_ACF.1.4/**AK.**VSDM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*][440].

Anwendungshinweis 190: Das Subjekt S_VSDD_Fachdienst vermittelt die Kommunikation des VSDD über den TLS-Kanal zwischen S_AK und VSDM-Intermediär. Das Subjekt S_CMS vermittelt die Kommunikation des CMS über den TLS-Kanal zwischen S_AK und VSDM-Intermediär.

FMT_MSA.1/AK.VSDM	**Management of security attributes / VSDM**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.
FMT_MSA.1.1/**AK.**VSDM	The TSF shall enforce the *VSDM-SFP*[441] to restrict the ability to [change_default, query, modify][442] the security attributes

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

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

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

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

[441] [assignment: *access control SFP(s), information flow control SFP(s)*]

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

	[*Konfigurationsparamter nach Tab_FM_VSDM_14 in [37]*] to *S_Administrator*.[443]

FMT_MSA.3/AK.VSDM	**Static attribute initialisation / VSDM**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/**AK.**VSDM	The TSF shall enforce the *VSDM-SFP*[444] to provide restrictive[445] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/**AK.**VSDM	The TSF shall allow the *S_Administrator*[446] to specify alternative initial values to override the default values when an object or information is created.

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

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

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

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

6.3.3.10. Übergreifende Sicherheitsanforderungen

FMT_MSA.4/AK	**Security attribute value inheritance**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

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

(1) *Der Chipkartendienst erzeugt für jede neu gesteckte Chipkarte*

(a) für identifizierte KVK,

(b) für identifizierte eGK, SMC und HBA

ein Kartenhandle und übergibt das Kartenhandle und die damit verknüpften Informationen an das Subjekt S_AK.

(2) Der Chipkartendienst öffnet auf Anforderung des Subjekts S_AK für eine mit dem Kartenhandle identifizierten Chipkarte einen logischen Kanal.

(3) Die TSF weisen

(a) vom EVG importierten zu signierenden Daten,

(b) vom EVG importierten zu verschlüsselnden Daten,

(c) vom EVG zu entschlüsselnden Daten,

(d) dem vom EVG identifizierten Subjekt „S_Benutzer_Clientsystem“

die vom EVG übergebene Identität und den Autorisierungsstatus „nicht autorisiert“ zu.

(4) Die TSF weisen nach erfolgreicher Prüfung der Signatur-PIN der Signaturchipkarte des identifizierten Benutzers des Clientsystems dem Autorisierungsstatus des Subjektes S_Benutzer_Clientsystem den Wert „autorisiert“ zu.

(5) Die TSF weisen den zu signierenden Daten einer Liste nach erfolgreicher Prüfung der Signatur-PIN der Signaturchipkarte des S_Benutzer_Clientsystem den Autorisierungsstatus „autorisiert“ zu.

(6) Der AK setzt den Wert des Sicherheitsattributes „Ordnungsgemäßigkeit der Signatur“ aller signierten Daten eines autorisierten Signaturstapels, der von der QSEE gesendet wird, auf „ordnungsgemäß“, falls folgendes gilt:

(a) Das S_Benutzer_Clientsystem hat während der Signaturerstellung keinen Abbruch der Signatur gefordert.

(b) Die TSF empfangen für jedes Kommando zur Signaturerzeugung einen erfolgreichen Rückkehrcode der QSEE.

(c) Die Anzahl der signierten Dokumente entspricht der Anzahl der zum Signieren übersandten Dokumente des autorisierten Stapels.

(d) Die qualifizierten elektronischen Signaturen für alle Elemente des autorisierten Signaturstapels werden vom EVG erfolgreich mit dem zum festgelegten Zeitpunkt gültigen qualifizierten Zertifikat des Benutzers des Clientsystems verifiziert.

(e) Die qualifizierten elektronischen Signaturen beziehen sich auf den vorher identifizierten Benutzer des Clientsystems und die Daten des autorisierten Signaturstapels.

(f) Die Freischaltung der QSEE für die Erstellung von qualifizierten elektronischen Signaturen wurde von dem EVG erfolgreich zurückgesetzt **falls nicht die Komfortsignatur-Funktion verwendet wird**.[447]

Sollte einer dieser Punkte nicht erfüllt sein, erhalten alle signierten Dokumente, die durch die aktuelle Signatur-PIN-Eingabe autorisiert wurden, das Attribut „ungültig“.

(7) Der EVG weist den Wert des Sicherheitsattributes „Ordnungsgemäss verschlüsselt“ verschlüsselter Daten nur dann auf „ordnungsgemäß“, wenn

(d) die identifizierte Verschlüsselungsrichtlinie für die zu verschlüsselnden Daten gültig ist,

(e) zu den vorgesehenen Empfängern gültige Verschlüsselungszertifikate existieren und für die Verschlüsselung des symmetrischen Schlüssels verwendet wurden,

(f) die durch den Xpath-Ausdruck selektierten zu verschlüsselnden Daten vollständig verschlüsselt wurden und

(g) keine Fehler auftraten.

.[448]

Anwendungshinweis 191: Die Zuweisung in der Regel (5) erfolgt in Übereinstimmung mit den Zugriffsregeln der qualifizierten Signaturerstellungseinheit. Für die Stapelsignatur nach TR-03114 [21] ist es notwendig, dass

- die QSEE nach einmaliger erfolgreicher Authentisierung des Signaturschlüssel-Inhabers die Erzeugung einer begrenzten Anzahl n ($n>1$) Signaturen erlaubt (mehrfachsignaturfähige QSEE),
- der EVG die berechtigt signierende Person durch die QSEE authentisiert und für das Signieren eines Stapels von m ($1 \leq m \leq n$) durch die QSEE autorisiert,

[447] Refinement: **falls nicht die Komfortsignatur-Funktion verwendet wird**

[448] [assignment: *rules for setting the values of security attributes*]

- der EVG nur die von der berechtigt signierenden Person übergebenen Dateien (Stapel) zeitlich zusammenhängend der QSEE zuführt und
- der EVG die Autorisierung des Signaturschlüssel-Inhabers nach dem Signieren dieses Stapels zurücksetzt.

Wenn die Anzahl der zu signierenden Daten größer ist als die zulässige Anzahl der nach einer Authentisierung mit der PIN.QES durch den HBA erstellbaren Signaturen, d.h. $m>n$, so soll der EVG den Benutzer Clientsystem zu erneuten Signatur-PIN-Eingabe für die nächsten maximal *n* zu signierenden Dateien auffordern bis der Stapel abgearbeitet ist. Die Signaturerstellung für die zu signierenden Daten eines autorisierten Stapels ist damit ein zeitlich zusammenhängender Prozess. Die Regel (6) des Elements FMT_MSA.4/**AK**.1 setzt die Forderung der TR-03114 [21], Schritt 4, dadurch um, dass in den aufgeführten Fällen alle bisher erstellen Signaturen des autorisierten Stapels verworfen und der Signaturprozess abgebrochen werden muss.

Wenn der Benutzer einen Abbruch des Signaturvorganges anfordert, so werden die vorher für den autorisierten (Teil-) Signaturstapel erstellten Signaturen verworfen und gelöscht und die Erzeugung der noch ausstehenden Signaturen wird abgebrochen. Wenn bei einer erneuten Signatur-PIN-Eingabe des Stapels ein Fehler auftritt (z. B. die zulässige Zeit für die PIN-Eingabe überschritten wird oder die PIN-Eingabe falsch ist), so soll dies wie ein vom Benutzer geforderter Abbruch behandelt werden.

In PP-0098 wird das SFR FMT_MSA.4/AK für die in dem PP beschriebenen Signaturarten „Einzelsignatur“ und „Stapelsignatur“ modelliert. Der EVG unterstützt zusätzlich die „Komfortsignatur“. Der Anwendungshinweis 191 des PP erlaubt ausdrücklich, dass für weitere Signaturarten teilweise von der Definition der SFR abgewichen werden kann. Insbesondere wird dabei FMT_MSA.4./AK Regel (6)(f) genannt.

Die Komforsignatur setzt diese Regel wie folgt um: Bei aktivierter Komfortsignatur wird die Zurücksetztung der Freischaltung des QSEE nicht durchgeführt.

Die Komfortsignatur ist per Default auf „Disabled“ (SAK_COMFORT_SIGNATURE=Disabled) gesetzt. Bevor die Komfortsignaturfunktion eingeschaltet werden kann müssen die Werte ANCL_TLS_MANDATORY und ANCL_CAUT_MANDATORY beide auf „Enabled“ stehen (TIP1-A4680-03). Bei der Komfortsignatur wird zwingend eine SecureMessaging (gSMC-K <-> HBA) benutzt (siehe FIA_UAU.5.2/AK (8) und und FIA_API.1/AK) (A_19258). Die Komfortsignaturfunktion kann durch den Befehl DeactiveComfortSignature oder durch das setzen von SAK_COMFORT_SIGNATURE auf „Disable“ global deaktiviert werden. Dadurch wird auch der Status aller HBAs bzw. HBA-Kartensitzungen zurückgesetzt (A_19105). Es werden vom EVG keine weiteren Signaturarten umgesetzt.

FDP_RIP.1/AK	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1/AK	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[449] the following objects:

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

(1) geheime kryptographische Schlüssel,
(2) zu signierende Daten,
(3) signierte Daten (nach der Ausgabe),
(4) zu verschlüsselnde Daten (nach der Verschlüsselung),
(5) verschlüsselte Daten (nach der Ausgabe),
(6) vorgeschlagene Empfänger,
(7) entschlüsselte Daten (nach der Ausgabe),
(8) Benutzerdaten, die über den TLS-Kanal zwischen EVG und eHealth-Kartenterminals übermittelt wurden
.[450]

Daten einer eGK dürfen nicht über den Steckzyklus der Karte hinaus im EVG gespeichert werden. Daten von HBA und SM-B dürfen nicht länger als 24 Stunden im EVG zwischengespeichert werden.

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

Anwendungshinweis 192: Beim Ziehen einer Chipkarte sowie beim Entfernen eines Kartenterminals werden eventuell vorhandene Puffer-Inhalte (Cache) sicher gelöscht.

6.3.4. Klasse FMT: Sicherheitsmanagement

FMT_SMR.1/AK	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1/**AK**	The TSF shall maintain the roles

(1) Administrator,
(2) Benutzer des Clientsystems,
(3) HBA,
(4) gSMC-KT, PIN-Sender,
(5) SMC-B,
(6) eGK,
(7) Kartenterminal,
(8) CMS of the gSMC-K ,
(9) Clientsystem,
(10) Fachmodul,
(11) *Fachdienst*

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

[451].

FMT_SMR.1.2/**AK**	The TSF shall be able to associate users with roles.
FMT_SMF.1/AK	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies..
FMT_SMF.1.1/**AK**	The TSF shall be capable of performing the following management functions: *(1) Manage eHealth-Kartenterminals according to FMT_MTD.1/AK.eHKT_**Abf** and FMT_MTD.1/AK.eHKT_**Mod**,* *(2) Manage Arbeitsplatzkonfiguration with assigned Clientsystems and eHealth-Kartenterminals according to FMT_MTD.1/AK.**Admin**,* *(3) Manage Signaturrichtlinien according to FMT_MSA.3/AK.**Sig**,* *(4) Manage TLS-Kanäle according to FMT_MSA.3/AK.**TLS**,* *(5) Manage Cross-CVC according to FMT_MTD.1/AK.**Zert**,* *(6) Management of TSF functions according to FMT_MOF.1/**AK*** *(7) Manage configuration parameters of Fachmodule* .[452]
FMT_MOF.1/AK	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1/AK	The TSF shall restrict the ability to <u>disable and enable</u>[453] the functions *Online Kommunikation, Signaturdienst und Logische Trennung*[454]to *Administrator*[455]. **The following rules apply:**

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

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

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

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

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

1. **If the attribute MGM_LU_ONLINE is set to “Disabled”, the Konnektor never establishes an online connection. This means, the following services are deactivated in this case:**
   (1) **Zertifikatsdienst: The TSL will be activated without evaluation of the revocation status (see FPT_TDC.1/AK).**
   (2) **TLS connection for Fachdienste: no TLS communication according to FTP_ITC.1/AK.FD.**
   (3) **Zeitdienst: time synchronization according to FPT_STM.1/NK.**
   (4) **Software-Aktualisierungsdienst: no communication with the update server according to FDP_ACF.1.4/Update.**
2. **If the attribute MGM_LU_SAK is set to “Disabled”, the Signaturdienst for QES according to the chapters 6.3.1.3 and 6.3.3.4 is deactivated.**
3. **If the logical separation is activated (attribute MGM_LOGICAL_SEPARATION set to “Enabled”), the following rules apply:**
   (1) **If invoked from an external interface, the Verschlüsselungsdienst of the Konnektor must not check the revocation status of certificates.**
   (2) **If invoked from an external interface, the Signaturdienst of the Konnektor must not check the revocation status of certificates.**
   (3) **IF MGM_LU_ONLINE is not enabled, the NTP server of the Konnektor must be deactivated.**
   (4) **If MGM_LU_ONLINE is set to “Enabled”, the Konnektor may only resolve the namespace „TI (*.DNS_TOP_LEVEL_DOMAIN_TI) “ for internal services and internal Fachanwendungen and must not resolve this namespace for requests originatred from the LAN.**
   (5) **The Konnektor must block all communication on its external interfaces with the following systems:**
      a. **with systems in the network segment ANLW_AKTIVE_BESTANDSNETZE initiated by „Aktive Komponenten“,**
      b. **with the Internet via SIS and IAG.**

Anwendungshinweis 193: Wenn MGM_LU_ONLINE=Disabled gesetzt ist, so baut der Konnektor grundsätzlich keine Online-Verbindungen zum WAN auf und beendet bestehende Kommunikation einschließlich VNP-Client, vergl. FMT_MSA.1/NK. Wenn MGM_LU_ONLINE=Enabled, aber MGM_LOGICAL_SEPARATION=Enabled, dann verhalten sich definierte Teile des Konnektors analog zu einer Auftrennung der Online-Verbindungen.

Anmerkung 9. Der EVG setzt die Funktionalität der logischen Separierung nicht um. Der EVG verhält sich dauerhaft wie ein Konnektor im Zustand MGM_LOGICAL_SEPARATION=disabled.

FMT_MTD.1/AK.Admin	**Management of TSF data / Adminstration**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/**AK.**Admin	The TSF shall restrict the ability to (1) *set*, query, modify and delete[456] the *roles from other users*[457], **(2) set, modify and delete[458] the authentication credentials for administrators[459],** **(3) set and modify[460] the Arbeitsplatzkonfiguration with assigned Clientsystem and eHealth-Kartenterminals[461],** **(4) set and modify[462] the Zeitpunkten und Gültigkeitsdauer der Prüfungsergebnisse zur Gültigkeit qualifizierter Zertifikate für die Erzeugung ordnungsgemäßer qualifizierten elektronischen Signaturen[463],** **(5) change_default[464] of the gültigen Signaturrichtlinie für Signaturerzeugung[465],** **(6) change_default[466] of the gültigen Signaturrichtlinie für Signaturprüfung[467],** **(7) modify[468] the configuration parameter to activate or deactivate the automatic installation of software updates[469],**

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

[457] [assignment: *list of TSF data*]

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

[459] [assignment: *list of TSF data*]

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

[461] [assignment: *list of TSF data*]

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

[463] [assignment: *list of TSF data*]

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

[465] [assignment: *list of TSF data*]

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

[467] [assignment: *list of TSF data*]

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

[469] [assignment: *list of TSF data*]

(8) import[470] the update data for Karten-Terminals and execute the update[471],

(9) configure[472] the loggable system events[473],

(10) export and import[474] the configuration data of the TOE[475],

(11) set and modify[476] the maximum lifetime of OCSP cache entries[477]

(12) set and modify[478] the keys of the sicheren Datenspeichers[479],

(13) set and import[480] the X.509 certificates of Clientsystemen[481],

(14) reset to factory settings[482] of ~~the~~ all TSF data (factory reset)[483],

(15) import[484] the CA certificates of an encryption PKI[485],

(16) generate, set, import, export and modify the used Konnektor certificate for client system TLS communication[486]

to *administrator*[487].

Für den Fall, dass die Remote-Managementschnittstelle verwendet wird, sind die Einschränkungen der Rechte aus TAB_KON_655 und TAB_KON_851 in [27] **zu berücksichtigen. Insbesondere können die Funktionen (1),**

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

[471] [assignment: *list of TSF data*]

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

[473] [assignment: *list of TSF data*]

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

[475] [assignment: *list of TSF data*]

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

[477] [assignment: *list of TSF data*]

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

[479] [assignment: *list of TSF data*]

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

[481] [assignment: *list of TSF data*]

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

[483] [assignment: *list of TSF data*]

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

[485] [assignment: *list of TSF data*]

[486] Refinement: (16) …

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

(2), (9), (10), (11), (12), (13), (14) und (15) nicht aufgerufen werden.

Anwendungshinweis 194: Der EVG authentisiert nur menschliche Benutzer in der Administrator-Rolle. Die TSF unterstützen das Erzeugen und den Export selbsterstellter X.509-Zertifikaten für Clientsysteme (s. FCS_CKM.1/NK.Zert) und den Import nicht durch die TSF erzeugter X.509-Zertifiakte für die Clientsysteme zur Kommunikation über einen TLS-Kanal (s. FTP_ITC.1/CS). Nach [110] sollen aber nur vom EVG erzeugte X.509-Zertifikaten für Clientsysteme verwendet werden.
Im Rahmen der interne Generierung oder Import eines Zertifikates/Schlüsselpaares für den EVG gibt es die Möglichkeit für den Adminstrator zwischen diesen Zertifikaten (C.AK.AUT, ID.AK.AUT, und auch dem ursprünglichen auf der gSMC.K) zu wechseln. Bei der Erstellung eines Schlüsselpaars und des X.509 Zertifikates hat der Administrator die Möglichkeit die kryptographischen Verfahren RSA-2048 oder ECC-256 auszuwählen (A_21699). Bei EVG Zertifikaten hat der Administrator auch die Möglichkeit den Hostnamen des Konnektors im Zertifikat zu vergeben. Ein in erneuertes C.AK.AUT wird nicht automatisch vom EVG verwendet (A_21759).

Anwendungshinweis 195: Regel (7) von FMT_MTD.1.1/AK.Admin wird duch die Auto-Update Funktion unterstützt.

FMT_MTD.1/AK.Zert	**Management of TSF data / Zertifikatsmanagement**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/**AK.**Zert The TSF shall restrict the ability to

(1) delete[488] the *public keys of the CVC root CA*[**489**] to *the CMS of the gSMC-K*[490],

(2) **import and permanently store[491] the public keys of the CVC root CA by the use of cross CVC[492] to S_AK[493].**

6.3.5. Klasse FPT: Schutz der TSF

FPT_TDC.1/AK	**Inter-TSF basic TSF data consistency**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

[489] [assignment: *list of TSF data*]

[490] [assignment: the authorised identified roles]

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

[492] [assignment: *list of TSF data*]

[493] [assignment: the authorised identified roles]

FPT_TDC.1.1/**AK** The TSF shall provide the capability to consistently interpret

(1) Zertifikate für die Prüfung qualifizierter elektronischer Signaturen,

(2) nicht-qualifizierter X.509-Signaturzertifikate,

(3) X.509-Verschlüsselungszertifikate,

(4) CV-Zertifikate,

(5) Trust-service Status Listen und TSL Hash-Werte,

(6) Certificate Revocation Listen,

(7) BNetzA-VL und BNetzA-VL Hashwerten,

(8) Zulässigkeit importierter zu signierenden bzw. zu prüfender signierten Daten gemäß implementierten Signaturrichtlinien,

(9) *[**NFDM** Signaturrichtlinie]*
[494]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/**AK** The TSF shall use *the following rules*

(1) Zertifikate für die qualifizierte elektronische Signatur müssen erfolgreich gemäß Kettenmodell bis zur bekannten und verifizierten BNetzA-VL erfolgreich geprüft sein.

(2) Die digitale Signatur der BNetzA-VL muss erfolgreich mit dem in der TSL enthaltenen öffentlichen Schlüssel zur Prüfung der BNetzA-VL geprüft sein und ist nur im angegebenen Gültigkeitszeitraum anwendbar. Die zeitliche Gültigkeit der BNetzA-VL muss erfolgreich geprüft werden.

(3) Die Gültigkeit der X.509-Signaturzertifikate der SMC-B gemäß [36] muss gemäß Schalenmodell bis zu einem gültige CA-Zertifikat der ausstellenden (zugelassenen) CA, das in einer gültigen TSL enthalten ist, erfolgreich geprüft sein.

(4) Die Gültigkeit der X.509-Verschlüsselungszertifikate gemäß Schalenmodell bis zu einem gültige CA-Zertifikat der ausstellenden (zugelassenen) CA, das in einer gültigen TSL enthalten ist, erfolgreich geprüft sein.

(5) Die Gültigkeit der CVC gemäß [15] muss nach dem Schalenmodell bis zu einer bekannten Wurzelinstanz erfolgreich geprüft sein.

(6) Die digitale Signatur über der TSL muss erfolgreich mit dem öffentlichen Schlüssel zur Prüfung von TSL erfolgreich geprüft sein und ist nur im angegebenen Gültigkeitszeitraum anwendbar. **Sollte die TSL über das Internet geladen werden muss der Konnektor zunächst die detachted-Signatur der TSL prüfen, einschließlich vollständiger Prüfung der Zertifikatskette bis zum TI-Vertrauensanker.** [495]

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

[495] Refinement: **Sollte die TSL …**

(7) Die digitale Signatur über der Certificate Revocation List muss mit dem öffentlichen Schlüssel zur Prüfung von CRL erfolgreich geprüft sein.

(8) Ein neuer öffentlicher Schlüssel zur Prüfung von TSL, CRL und BNetzA-VL darf nur durch eine gültige TSL verteilt werden.

(9) *[für NFDM Signaturrichtlinie die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen]*.[496]

when interpreting the TSF data from another trusted IT product.

Anwendungshinweis 196: Die Vertrauenswürdigkeit des IT-Produktes, von dem TSF-Daten importiert werden, ergibt sich aus einer gültigen digitalen Signatur, die mit den im EVG vorhandenen öffentlichen Schlüsseln der bekannten Vertrauensanker ggf. in einer Zertifikatskette erfolgreich geprüft werden konnte. Die „Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen“ ist gegeben, wenn (i) die Signaturrichtlinie keine qualifizierte elektronische Signatur fordert, oder (ii) die Signaturrichtlinie eine qualifizierte elektronische Signatur und die in diesem ST für qualifizierte elektronische Signaturen definierten Regeln gemäß FDP_ACF.1/AK.**Sgen**, FDP_ACF.1/AK.**SigPr**, FDP_DAU.2/AK.**QES** und FDP_DAU.2/AK.**Cert** einhält.

Die in der letzten Regeln von FPT_TDC.1.2 genannten Signatursrichtlinien (zu unterstützende Dokumenten- / Signatur-formate und XML-Daten-Interpretationsvorschriften) werden im Zuge von Updates des EVG (z. B. beim Einbringen neuer Fachmodule) importiert. Die Signaturprüfung erfolgt dann implizit durch die Signaturprüfung des Update-Pakets entsprechend FDP_ACF.1/AK.**Update**.

Anwendungshinweis 197: Die BNetzA-VL wird gemäß Anforderung A_6730 der Konnektor-Spezifikation [27] im Online-Modus mindestens einmal täglich auf Aktualität überprüft. Der EVG interpretiert den Hash-Wert der BNetzA-VL gemäß Use Case TUC_KON_031 der Konnektor-Spezifikation [27].

Anmerkung 10. Der Konnektor ermöglicht den Import des TSL-Signer-CA Cross-Zertifikats auch, wenn er sich im kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period befindet (**A_17549-01**).
Um auf Basis des bereits etablierten Vertrauensankers (RSA) in den Vertrauensraum (ECC-RSA) zu wechseln verwendet der Konnektor bei der Initialisierung des neuen Vertrauensankers (ECC-RSA) Cross-Zertifikate. Das Ergebnis ist ein neuer etablierter TI-Vertrauensanker (ECC-RSA) (**A_17837-01**), der im sicheren Speicher abgelegt wird (**A_17548-01**).
Es wird vom Konnektor ein Vergleich des PublicKey im Cross-Zertifikat mit dem PublicKey im CA-Zertifikat des neuen Vertrauensankers (TSL-Signer-CA<X>) durchgeführt. Dabei wird eine Signatur-Prüfung des Cross-Zertifikates gegen den alten

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

Vertrauensanker im System (TSL-Signer-CA<Y>) durchgeführt analog zu TUC_PKI_004. Die neue TSL (passend zum Vertrauensanker TSL-Signer-CA<X>) wird analog zu GS-A_4748 eingebracht und danach das Element TSLSequenceNumber ausgelesen. Falls für den TSLSequenceNumber-Nummernkreis der neu eingebrachten TSL eine TSLSequenceNumber im sicheren Speicher vorliegt, dann muss die TSLSequenceNumber der neu eingebachten TSL höher sein, als dieser Wert. Wenn einer der Schritte fehlschlägt, wird der Vertrauensraum-Wechsel-Prozess abgebrochen und der alte Vertrauensanker (TSL-Signer-CA<Y>) verbleibt im Konnektor. (**A_17821**)
Der Konnektor sichert für den Download der Hash-Datei der TSL(ECC-RSA) die Verbindung zum TSL-Dienst durch TLS ab. Der Konnektor prüft das vom TSL-Dienst beim TLS-Verbindungsaufbau präsentierte Zertifikat C.ZD.TLS-S. Die Prüfung erfolgt durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ {
certificate = C.ZD.TLS-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_zd_tls_s; intendedKeyUsage = intendedKeyUsage(C.ZD.TLS-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP } .
Falls Fehler im TLS-Verbindungsaufbau bzw. bei der Zertifikatsprüfung auftreten MUSS der Konnektor den TLS-Verbindungsaufbau mit Fehlercode 4235 gemäß TAB_KON_825 abbrechen (**A_17661**).
Der Konnektor muss für die Prüfung der Signatur der TSL(ECC-RSA) das Signaturverfahren ECDSA auf Basis der Domainparameter brainpoolP256r1 verwenden mit dem XMLDSig-Identifier „ http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256“ mit entsprechenden TSL-Signer-CA-Zertifikat (ECDSA) (**A_17688**). Als Hashfunktion (Messagedigest) wird SHA-256 verwendet (**A_17205**).
Die TSL kann auch direkt aus dem Internet geladen werden, wenn sie in der TI nicht verfügbar ist (TIP1-A_4736-02). Hierbei wird zusätzlich die detachted Signature der TSL übertragen. Im Internet sind die TSL-Downloadpunkt des TSL Diensteservers erreichbar, siehe auch FDP_IFC.1/NK.PF (TIP1-A_4693-02).

FPT_FLS.1/AK	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1/**AK**	The TSF shall preserve a secure state **according to TAB_KON_504 [27]** when the following types of failures occur: *(1) according to TAB_KON_503 [27] with type „SEC“ and severity „fatal“.* *(2) [Error Condition EC_FW_Not_ Valid_Status_ Blocked according to [27]]* [497] [498].

[497] [assignment: *list of additional types of failures in the TSF*]

[498] [assignment: *list of types of failures in the TSF*]

Failures occured during the self test of the TOE (see FPT_TST.1/AK.Run-Time and FPT_TST.1/AK.Out-Of-Band) must trigger a blockage of the affected parts of the TSF.

Anwendungshinweis 198: Für dedizierte Fehlerarten unterbindet der EVG bestimmte weitere Funktionalität. Diese Fehlerarten und die erlaubten bzw. verbotenen Dienste sind in Tabelle TAB_KON_504 in [27] definiert. Insbesondere wird für *Error Condition EC_FW_Not_Valid_Status_ Blocked* TIP1-A_6025 nach [27] umgesetzt. Im Fehlerfall *EC_Firewall_Not_Reliable* deaktiviert der EVG die LAN- und WAN-Schnittstelle und lässt insbesondere keine administrativen Funktionen an diesen Schnittstellen zu.

Anwendungshinweis 199: Sonstige Fehlerzustände des EVG, die an dessen äußeren Schnittstellen auftreten, obliegen den funktionalen Tests zur Zulassung.

FPT_TEE.1/AK	**Testing of external entities**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TEE.1.1/**AK**	The TSF shall run a suite of tests

(1) *beim Herstellen einer Kommunikation mit einem Gerät, das vorgibt, ein eHealth-Kartenterminal zu sein*[499] to check the fulfillment of *das Gerät ist dem EVG als zulässiges eHealth-Kartenterminal im LAN des Leistungsrbringers bekannt, d. h. ein eHealth-Kartenterminal mit dem Pairing-Geheimnis und der beim Pairing gesteckten gültigen gSMC-KT.*[500]

(2) bei der Meldung eines eHealth-Kartenterminals über das Stecken einer Chipkarte[501] **to check the fulfillment of:**

(a) die gesteckte Chipkarte ist eine KVK.

(b) Die Chipkarte ist eine Chipkarte des identifizierten Kartentyps eGK, HBA, gSMC-KT oder SMC-B und keine KVK. [502]

(3) bei entfernter Eingabe von PIN- oder PUK[503] **to check the fulfillment of:**

(a) Zulässigkeit mit dem CVC mit Flag '54' für die Nutzung einer gSMC-KT als PIN-Sender für die entfernte PIN-Eingabe.

(b) Zulässigkeit für einen HBA oder einer SMC-B mit dem

[499] [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

[500] [assignment: *List of properties of the external entities*]

[501] [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

[502] [assignment: *List of properties of the external entities*]

[503] [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

CVC Flag ’55’ für die Nutzung einer Chipkarte als PIN-Empfänger für die entfernte PIN-Eingabe.

• [504]

FPT_TEE.1.2/**AK** If the test fails, the TSF shall

(1) keine weitere Kommunikation mit dem Gerät aufzunehmen und eine Fehlermeldung an den EVG zu geben.

(2) wenn für eine Chipkarte die Testfolge des identifizierten Kartentyps, der keine KVK ist, fehlschlägt, ist der angeforderte Prozess abzubrechen und eine Fehlermeldung an den EVG zu geben.

(3) wenn die gesteckte Chipkarte nicht als KVK, eGK, HBA, gSMC-KT oder SMC-B identifiziert werden kann, soll die TSF [den angeforderten Prozess auf der Chipkarte abbrechen und eine Fehlermeldung zurück geben] [505].

[506]

Anwendungshinweis 200: Wenn keine weiteren Chipkarten unterstützt werden, ist eine Fehlermeldung an den EVG über einen unbekannten Kartentyp zu übergeben. Die Testfolge für ein eHealth-Kartenterminal besteht in dem Aufbau eines TLS-Kanals mit Prüfung des Zertifkats einer gültigen gSMC und des Pairing-Geheimnis (s. [38]). Die Testfolge für eine KVK besteht im Lesen und Auswerten des ATR der Chipkarte. Die Testfolge für Chipkarten des Kartentyps eGK, HBA, gSMC-KT und SMC-B umfasst die sichere Bestimmung der Karte und des Kartentyps.

FPT_TST.1/AK.Run-Time	**TSF testing / Normalbetrieb**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1/**AK.**Run-Time	The TSF shall run a suite of self tests *beim Anlauf und regelmäßig während des Normalbetriebs*[507] to demonstrate the correct operation of [*TLS, AES*][508].
FPT_TST.1.2/**AK.**Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of [*the following parts of TSF data:*

[504] [assignment: *list of properties of the external entities*]

[505] [assignment: *action(s)*]

[506] [assignment: *action for unknown smart card*]

[507] [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]*]

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

- *CRL*][509].

FPT_TST.1.3/**AK.**Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of [*TLS, AES*][510].

Anwendungshinweis 201: Die Komponente FPT_TST.1.1/Run-Time fordert den Selbsttest des EVG unter normalen Betriebsbedingungen, d. h. beim Anlauf (z. B. Einschalten des Konnektors) und während des Normalbetriebs. Die Selbsttests zu AES beinhalten Tests zum korrekten Aufruf der AES Routinen des Kernels. Wenn AES-NI aktiviert ist, wird entsprechend der HW-Aufruf des AES-Algorithmus von den Selbsttests geprüft. Für die TLS Selbstests wird ein TLS Server und ein TLS Client initialisiert und daraufhin mit verschiedenen Cipher Suites ein TLS Handshake ohne Authentisierung des TLS Clients untereinander durchgeführt. Die Integrität der CRL wird beim Anlauf und während des Normalbetriebs vor jeder Verwendung geprüft.

FPT_TST.1/AK.Out-Of-Band	**TSF testing / Out-Of-Band**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1/**AK.**Out-Of-Band	The TSF shall run a suite of self tests **durch TSF-Komponenten mit integritätsgeschützt gespeichertem Code** *beim Erstanlauf und auf Anforderung eines autorisierten Benutzers*[511] to demonstrate the correct operation of the TSF[512].
FPT_TST.1.2/**AK.**Out-Of-Band	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[513].
FPT_TST.1.3/**AK.**Out-Of-Band	The TSF shall provide authorised users with the capability to verify the integrity **des gespeicherten ausführbaren Codes** of [*none*][514].

Anwendungshinweis 202: Dieses SFR wird durch den Sicheren Start-Up umgesetzt, siehe 7.1.5 NK.Selbstschutz. Der Vertrauensanker ist Intergritätsgeschützt im BIOS abgelegt. Durch Neustart kann der Benutzer den Selbstest jederzeit anstossen.

FPT_STM.1/AK	**Reliable time stamps**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

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

[511] [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]*]

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

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

[514] [assignment: *parts of TSF **mit gespeichertem ausführbarem TSF-Code***]

FPT_STM.1.1/AK	The TSF shall be able to provide reliable time stamps **für vom AK erzeugte Protokolleinträge (gemäß FAU_GEN.1/AK)**. **Der AK greift auf die Echtzeituhr zurück, die in regelmäßigen Abständen und auf Anforderung des Administrators vom NK mit einem vertrauenswürdigen Zeitdienst synchronisiert wird.**

EVG Ausstrahlung

Maßnahmen zur Verhinderung von kompromittierenden Informationen in Signalen über die äußeren Schnittstellen des EVG sind einerseits in FPT_EMS.1/NK gefordert. Darüber hinaus werden sie als Bestandteil der Sicherheitsarchitektur des EVG (vgl. die Vertrauenswürdigkeitskomponente ADV_ARC.1) angesehen. Die Sicherheitsarchitekturbeschreibung beschreibt bzw. demonstriert, durch welche Maßnahmen der Selbstschutz, die Domain-Separierung und die Nichtumgehbarkeit der Sicherheitsfunktionalität realisiert ist [6].

6.3.6. Klasse FAU: Sicherheitsprotokollierung

FAU_GEN.1/AK	**Audit data generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1/AK	The TSF shall be able to generate an audit record of the following auditable events **des Anwendungskonnektors**: a) Start-up and shutdown of the audit functions **des Anwendungskonnektors**; b) All auditable events for the [not specified][515] level of audit; and *c) The following specified security-relevant auditable events:* • *Power on / Shut down (einschließlich der Art der ausgelösten Aktion, z. B. Reboot) des Anwendungskonnektors,* • *Durchführung von Softwareupdates einschließlich nicht erfolgreicher Versuche des Anwendungskonnektors,* • *Zeitpunkt von Änderungen der Konfigurationseinstellungen und Export/Import von Konfigurationsdaten des Anwendungskonnektors,* • *kritische Betriebszustände wie in der Tabelle in FPT_FLS.1/AK aufgelistet des Anwendungskonnektors,* • *Ereignisse vom Typ „Sec“ des Anwendungskonnektors,* • *[none]*[516] [517].

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

[516] [assignment: *additional events*]

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

FAU_GEN.1.2/AK	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each **specified** audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*][518].

Anwendungshinweis 203: FAU_GEN.1/AK beschreibt die Protokollfunktionen des Anwendungskonnektors in Ergänzung zu FAU_GEN.1/NK.SecLog. Die Protokoll-Daten dürfen keine personenbezogenen oder medizinischen Daten enthalten. Die Spezifikation Konnektor [27] gibt im Anhang F eine Übersicht der Ereignisse (Events) und im Anhang G eine Übersicht der Fehlercodes, wobei nur die Beschreibungen der Ereignisse und Fehlercodes für die jeweiligen Technischen Anwendungsfälle (TUC) verbindlich sind.

FAU_SAR.1/AK	**Audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1/AK	The TSF shall provide [*the administrator*][519] with the capability to read [*audit data according to FAU_GEN.1.1/NK and FAU_GEN.1.1/AK*][520] from the audit records.
FAU_SAR.1.2/AK	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1/AK	**Protected audit trail storage**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1/AK	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2/AK	The TSF shall be able to prevent[521] unauthorised modifications to the stored audit records in the audit trail.

Anwendungshinweis 204: Entsprechend [27] ist kein Nutzer befugt, Modifizierungen der Protokollaufzeichnungen vorzunehmen. Der Protokollspeicher kann weit über 10.000 Einträge aufnehmen; ältere Einträge werden rollierend überschrieben.

[518] [assignment: *other audit relevant information*]

[519] [assignment: *authorised users*]

[520] [assignment: *list of audit information*]

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

FAU_STG.4/AK	**Prevention of audit data loss**
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.4.1/AK	The TSF shall overwrite the oldest stored audit records[522] and [*raise Error Condition EC_LOG_OVERFLOW according to TAB_KON_503 [27]*][523] if the audit trail is full.

[522] [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

[523] [assignment: other actions to be taken in case of audit storage failure]

6.3.7. Sicherheitsanforderungen für die ePA Fachanwendung (PTV4)

6.3.7.1. VAU-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Anmerkung 11. Zur Absicherung der Kommunikation zwischen der VAU des ePA Aktensystems und dem Client (Konnektor mit ePA Fachmodul) wird das in [30], Kapitel 6, spezifizierte Kommunikationsprotokoll umgesetzt.

FTP_ITC.1/VAU	**Inter-TSF trusted channel VAU**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAU	The TSF shall provide a communication channel between itself and **~~another trusted IT product~~ der Vertrauenswürdigen Ausführungsumgebung (VAU)**[524] 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**[525] disclosure.
FTP_ITC.1.2/VAU	The TSF shall permit the TSF[526] to initiate communication via the trusted channel.
FTP_ITC.1.3/VAU	The TSF shall initiate communication via the trusted channel for *communication required by the ePA architecture for exchange of messages with the VAU*[527].

[524] refinement

[525] refinement (or → and)

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

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

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss als „leichtgewichtige Sicherungsschicht“ innerhalb eines TLS-Kanals aufgebaut werden (siehe gemSpec_Krypt [30] Kapitel 6). Die folgende Cipher Suite muss unterstützt werden:

AES-256-GCM-BrainpoolP256r1-SHA-256, mit

ECDH zum Schlüsselaustausch.

Der Anwendungskonnektor startet die Kommunikation mit VAUClientHello Nachricht und kann die Endstelle in Abhängigkeit von dem Serverzertifikat und der ServerHello Nachricht authentifizieren.

Anmerkung 12. Der Anwendungskonnektor muss die Regeln durchsetzen, die gemäß [30], Kapitel 6, für die vom Konnektor initiierten VAU-Verbindungen gefordert werden. Die Nachrichten werden entsprechend A_16884 per HTTP mit dem Content-Type 'application/json' oder 'application/octet-stream' übermittelt. Der Konnektor führt einen unsigned 64-Bit-Nachrichtenzähler, der bei jeder abgeschickten Nachricht (siehe A_16945-02) um zwei erhöht wird und einen KeyID-Zählerwert, welcher bei jeder erfolgreichen Nachricht um eins erhöht wird. Das komplette VAU Protokoll mit VAUClientHello (A_16903), VAUClientSigFin (A_17070-02, A_17071), VAUServerFin (A_17084) und VAUServerHelloData (A_16903, A_16941-01) ist aufgebaut wie beschreiben in A_16900 und folgende.

Bei jeder VAU-Verbindung vom Anwendungskonnetor stellt der Anwendungskonnetor sicher, dass:

- die Authentizierung für jeden Endpunkt durchgeführt wird.
- nur der Konnektor die VAU-Verbindung beginnen kann und bei der Verbinung eine VAUClientHello Nachricht laut A_16883-01 geschickt wird.
- zusätzliche (i. S. v. ihm unbekannte) Datenfelder (Key-Value-Paare) in JSON-Objekten (Typ-(1)-Nachrichten und "Data"-Feldern darin) im Rahmen des VAU-Protokolls werden vom Konnektor ignoriert. (A_17074)
- neue symmetrische Schlüssel generiert werden, wenn der unsigned 64-bit Zähler möglicherweise überläuft oder nach 24 Stunden.
- die Verbindung terminiert wird, wenn das Zertifikat nicht die OID oid_epa_vau (nach [50]) hat.

- Die Verbindung terminiert wird wenn die Abbruchbendingungen nach A_17084, A_16957-01, A_16900, A_16903 oder A_16941-01 gelten

FCS_CKM.1/VAU	**Cryptographic key generation / VAU**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/VAU.AES und FCS_COP.1/VAU.Auth [FCS_CKM.4 Cryptographic key destruction] hier erfüllt durch FCS_CKM.4/AK
FCS_CKM.1.1/VAU	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *VAU key agreement with ECDH and AES-256-GCM-BrainpoolP256r1-SHA-256.*[528] and specified cryptographic key sizes *256 bit for AES-256, 256 for ECDH*[529] that meet the following: *[*30*] (A_16943-01), FIPS PUB 180-4 [54], RFC-5869 [103], RFC 5639 [101].*[530]

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

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

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

FCS_COP.1/VAU.AES	**Cryptographic operation for VAU**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FCS_CKM.1/VAU FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/VAU.AES	The TSF shall perform *symmetric authenticated encryption and decryption*[531] in accordance with a specified cryptographic algorithm *AES-256 in GCM Mode with authentication tag length of 128 bit* [532] and cryptographic key sizes *256 bit for AES-256*[533] that meet the following: *FIPS 197 [55], NIST 800-38D [99], RFC 5116 [104], specification [30]* [534].

Anmerkung 13. Es gilt Anwendungshinweis 109. Der IV für den GCM Mode muss zufällig gewählt werden

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

[532] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/VAU.Auth	**Cryptographic operation for VAU**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] Die hier genannten Abhängigkeiten werden nicht erfüllt. Begründung: Die *signature creation* wird von der SMC-B oder eGK durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der Karte. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* kann auch im EVG durchgeführt werden. Die entsprechenden öffentlichen Schlüsselobjekte werden durch den Import von Zertifikaten in den EVG eingebracht, die Abhängigkeit wird inhaltlich durch FPT_TDC.1/SGDVAU erfüllt. FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.
FCS_COP.1.1/VAU.Auth	The TSF shall perform a) *verification of digital signatures and* b) *signature creation with support of eGK, SMC-B storing the signing key and performing the ECC operation* [535] in accordance with a specified cryptographic algorithm *ECDSA-with-Sha256 OID 1.2.840.10045.4.3.2 with curve brainpoolP256r1*[536] and cryptographic key sizes *256 bit*[537] that meet the following: *TR-03111 [23]*, *RFC 5639 [101]*, *FIPS PUB 180-4 [54]*[538].

Anmerkung 14. Die Signaturberechnung gemäß FCS_COP.1/VAU.Auth wird für die Berechnung digitaler Signaturen zur Authentisierung bei der VAU verwendet. Der EVG nutzt dafür bei Verbindungen zur VAU die AUT-Identity der SMC-B oder eGK. Der dafür benötigt asymmetrische Schlüssel kann während der Produktion der Chipkarte importiert oder generiert werden. Es werden deshalb keine spezifischen Anforderungen an die Quelle dieses Schlüssels gestellt.

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

[536] [assignment: *cryptographic algorithm*]

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

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

6.3.7.2. SGD-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Anmerkung 15. Zur Absicherung der Kommunikation zwischen den Schlüsselgenerierungsdiensten der ePA Fachanwendung (SGD1 und SGD2) und dem Client (Konnektor mit ePA Fachmodul) werden über das HTTPS-Interface Datenpakete ausgetauscht. Einzelne darin enthaltene Datenfelder, die direkt für das HSM des jeweiligen SGD bestimmt sind, werden durch ECIES-Verschlüsselung gesichert. Dabei handelt es sich nicht um einen Kommunikationskanal im eigentlichen Sinne. Dennoch wird der gesicherte Anteil der Kommunikation als „Kanal“ zwichen Client und SGD-HSM aufgefasst und im folgenden mit FTP_ITC.1/SGD (Analog zum VAU Kanal FTP_ITC.1/VAU) als trusted channel modelliert. So können gezielte Anforderungen an diese Kommunikation gestellt werden, siehe Refinement und Anmerkung zum SFR.

FTP_ITC.1/SGD	**Inter-TSF trusted channel SGD**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/SGD	The TSF shall provide a communication channel between itself and **~~another trusted IT product~~ dem Schlüsselgenerierungsdienst (SGD)**[539] 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**[540] disclosure.
FTP_ITC.1.2/SGD	The TSF shall permit the TSF[541] to initiate communication via the trusted channel.
FTP_ITC.1.3/SGD	The TSF shall initiate communication via the trusted channel for *communication required by the ePA architecture for exchange of messages with the SGD*[542].

[539] refinement

[540] refinement (or → and)

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

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

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss auf Basis des ECIES-Protokolls aufgebaut werden (siehe Spezifikation Schlüsselgenerierungsdienst ePA [48], Kapitel 9). Die folgenden kryptographischen Algorithmen MÜSSEN unterstützt werden:

BrainpoolP256r1, SHA-256 und AES-256-GCM für ECIES,

ECDSA für die Signatur.

Das ECIES-Schlüsselmaterial für den Kanal muss kryptographisch frisch sein und damit nach jedem erfolgreichen Kanal neu erzeugt werden, siehe A_18005.

Anmerkung 16. Der Anwendungskonnektor muss die Regeln durchsetzen, die gemäß der Spezifikationen [30] und [48] für die vom Konnektor initierten SGD-Verbindungen gefordert werden. Wenn der EVG unbekannte Key-Value Paare in JSON Nachrichten erhält, müssen diese in der Kommunikation ignoriert werden. Bei dem SGD Protokoll wird eine zufällige Challenge vom EVG erstellt, welche bei der Rückantwort auf Korrektheit geprüft wird.

Bei jeder SGD-Verbindung vom Anwendungskonnetor stellt der Anwendungskonnetor sicher, dass:

- die Authentizierung für jeden Endpunkt (SGD-HSM 1 und SGD-HSM 2) durchgeführt wird. Hierbei wird GetPublicKey (A_17897 und A_17899) als Funktion genutzt.
- nur der Konnektor die SGD-Verbindung beginnen kann.
- neue symmetrische Schlüssel für jeden Schlüsselableitungsrequest generiert werden (A_18005).
- die Kodierung des Chiffrat entsprechend A_17902 durchgeführt wird.
- die Anfragen sind entsprechend A_17924-01 aufgebaut.
- der Konnektor nimmt bei der zweiten Verschlüsselungsschicht die Associated Data (AD) der ersten Schicht (AD 1) im AD der zweiten Schicht (AD 2) mit auf. Der Konnektor führt zunächst AD 1 und dann AD 2 auf und trennt beide durch mindestens ein Leerzeichen. Die GMAC-Berechnung erfolgt bei der zweiten Verschlüsselung über beide AD (AD1 und AD2) (AD1 + AD2 bilden die AD für den AES-GCM). (A_17930)

- eine Prüfung der Telematik-ID wird laut A_18003 durchgeführt.
- die Variable KVNR wird vom Konnektor laut A_18006 interpretiert.
- der Konnektor prüft die Antwort auf eine „KeyDerivation“ entsprechend A_18031-01 und A_20977.
- die Verbindung terminiert wird, wenn das Zertifikat nicht die OID oid_SGD{1/2}_hsm (siehe A_17848 und [50]) und die korrekte Servicetypkennung („http://uri.etsi.org/TrstSvc/Svctype/unspecified“, siehe A_17847) hat. Bei der Prüfung des SGD-HSM-ECIES-Schlüssel gelten die Regeln für Abbrüche laut A_18024.
- die Schlüsselableitung laut A_17888 und A_17898 durchgeführt wird für SGD ePA unter Nutzung des zuvor erhaltenen Authentisierungstoken (Prüfung der Antwort des SGD auf GetAuthenticationToken entsprechend A_18028).
- der Konnektor prüft, ob im HTTP-Response-Header einer Antwortnachricht eine HTTP-Variable Namens "SGD-Userpseudonym" enthalten ist. Wenn dies der Fall ist führt der Konnektor diese Variable inkl. Wert unverändert im nächsten Request an den SGD im HTTP-Request-Header auf.

FCS_COP.1/SGD.ECIES	**Cryptographic operation for VAU**
Hierarchical to:	No other components.
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.2/SGD FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/SGD.ECIES	The TSF shall perform *ECIES based authenticated hybrid encryption and decryption with ECC key pair generation*[543] in accordance with a specified cryptographic algorithm *ECIES with brainpoolP256r1, HKDF with SHA-256 and AES-256 in GCM Mode with authentication tag length of 128 bit* [544] and cryptographic key sizes *256 bit for AES-256*[545] that meet the following: *SEC1-2009 [102], NIST-800-56-A [105], RFC 5639 [*101*], FIPS PUB 180-4 [54], RFC-5869 [*103*], FIPS 197 [55], NIST 800-38D [99], RFC 5116 [104], gemSpec_Krypt [30]* [546].

Anmerkung 17. Die Kodierung des "PublicKeyECIES" muss wie in A_17900 beschrieben geschehen. Die Behandlung der Signatur muss nach A_17901 geschehen. Der Konnektor prüft, ob der erhaltetene ephemeren ECC-Punkt auf der elliptischen Kurve liegt (A_17903).
Die Anfrage „GetAuthenticationToken“ wird mit einer 256 bit Zufallszahl (extern erzeugt) sowie eines „H-Wert“ (SHA-256 Hash über Client-ECIES-Schlüssel und AUT-Zertifikat) codiert wie in A_18025-01 beschrieben. Das erhaltene Chiffrat wird laut A_17902 kodiert und bei „GetAuthenticationToken“ (A_18021) verwendet.
Die Erzeugung der Anfrage „KeyDerivation“ wird entsprechend zu A_18029 vom Konnektor durchgeführt.

Anmerkung 18. Es gilt Anwendungshinweis 109. Der IV für den GCM Mode muss zufällig gewählt werden. Ein Chiffrat muss laut A_18004 kodiert werden.

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

[544] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/SGD.Auth	**Cryptographic operation for SGD**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] Die hier genannten Abhängigkeiten werden nicht erfüllt. Begründung: Die *signature creation* wird von der SMC-B oder eGK durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der Karte. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* kann auch im EVG durchgeführt werden. Die entsprechenden öffentlichen Schlüsselobjekte werden durch den Import von Zertifikaten in den EVG eingebracht, die Abhängigkeit wird inhaltlich durch FPT_TDC.1/SGDVAU erfüllt. FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.
FCS_COP.1.1/SGD.Auth	The TSF shall perform a) *verification of digital signatures and* b) *signature creation with support of SMC-B or eGK storing the signing key and performing the ECC operation* [547] in accordance with a specified cryptographic algorithm *ECDSA-with-Sha256 OID 1.2.840.10045.4.3.2*[548] and cryptographic key sizes *256 bit*[549] that meet the following: *TR-03111 [23]*, *RFC 5639 [101]*, *FIPS PUB 180-4 [54]*[550].

Anmerkung 19. Die Signaturberechnung gemäß FCS_COP.1/SGD.Auth wird für die Berechnung der digitaler Signaturen zur Authentisierung des eigenen ephemeren öffentlichen Schlüssels beim SGD verwendet (A_17900, A_17901 in [48] und A_17874 in [30]). Der EVG nutzt dafür bei Verbindungen zum SGD die SMC-B oder

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

[548] [assignment: *cryptographic algorithm*]

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

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

die eGK (bei Kontoeröffnung und Berechtigungsvergabe). Der Konnektor unterstützt auch G2.0 Karten bei denen ausschließlich RSA-Signatur-Verfahren möglich sind. Für G2.0 Karten wird das Signatur-Verfahren RSASSA-PSS mit SHA256 ([53]) für die Authentisierung des eigenen ephemeren öffentlichen Schlüssels beim SGD verwendet. Für Karten, die ECDSA- und RSA- Verfahren unterstützen (ab G2.1) wird vom Konnektor immer ECDSA für die Berechnung der Signaturen verwendet.

FDP_ITC.2/SGD	**Import of user data with security attributes / SGD-Client**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] hier erfüllt durch: FDP_ACC.1/SGD [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] hier erfüllt durch: FTP_ITC.1/SGD FPT_TDC.1 Inter-TSF basic TSF data consistency hier erfüllt durch: FPT_TDC.1/SGDVAU
FDP_ITC.2.1/**SGD**	The TSF shall enforce the *SGD-SFP*[551] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/**SGD**	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/**SGD**	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/**SGD**	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/**SGD**	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: (1) *Die TSF importiert über die Operation GetPublicKey den öffentlichen ECIES-Schlüssel eines SGD-HSMs.*[552]

FDP_ACC.1/SGD	**Subset access control / SGD-Client**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control hier erfüllt durch: FDP_ACF.1/SGD
FDP_ACC.1.1/**SGD**	The TSF shall enforce the *SGD-SFP*[553] on

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

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

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

the subject:

- *SGD-Client,*

the object:

- *öffentlicher ECIES-Schlüssel eines SGD-HSMs,*

and the operation:

- *ECIES-Encryption entsprechend FCS_COP.1/SGD.ECIES*

FDP_ACF.1/SGD	**Security attribute based access control / SGD-Client**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control hier erfüllt durch: FDP_ACC.1/SGD FMT_MSA.3 Static attribute initialisation nicht erfüllt mit folgender Begründung: Für das Datenobjekt *öffentlicher ECIES-Schlüssel eines SGD-HSMs* findet keine Initialisierung von Sicherheitsattributen im Sinne von FMT_MSA.3 statt: *ECIES-Schlüssel, Signatur und Zertifikat* können nicht sinnvoll vom EVG mit Default Werten initialisiert werden.
FDP_ACF.1.1/**SGD**	The TSF shall enforce the *SGD-SFP*[554] to objects based on the following: *subject:* • *SGD-Client* *objects:* • *öffentlicher ECIES-Schlüssel eines SGD-HSMs with the security attribute:* a. *Signatur* b. *Zertifikat*
FDP_ACF.1.2/**SGD**	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Der SGD-Client darf den öffentlicher ECIES-Schlüssel eines SGD-HSMs für ECIES-Encryption entsprechend FCS_COP.1/SGD.ECIES verwenden wenn die folgenden Bedingungen erfüllt sind (A_18024):* *(1) Das erhaltene Zertifikat des SGD-HSMs muss gemäß A_17847 gültig sein.* *(2) Das erhaltene Zertifikat des SGD-HSMs muss so wie vom Client erwartet entweder von einem SGD 1 oder von einem SGD 2 gemäß A_17848 sein.*

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

(3) Das erhaltene Zertifikat des SGD-HSMs muss zeitlich gültig sein.

(4) *Die Signatur muss eine kryptographisch korrekte Signatur, die auf den EE-Schlüssel des erhaltene Zertifikat rückführbar ist sein..*[555]

FDP_ACF.1.3/**SGD** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[556].

FDP_ACF.1.4/**SGD** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[557].

Anmerkung 20. Der „öffentlicher ECIES-Schlüssel eines SGD-HSMs“ und die entsprechenden Sicherheitsattribute „Signatur“ und „Zertifikat“ werden in der Response zum GetPublicKey-Request an den SGD-Client übermittels (A_17895-01 und A_17894-01)

FPT_TDC.1/SGDVAU	**Inter-TSF basic TSF data consistency**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1/ **SGDVAU**	The TSF shall provide the capability to consistently interpret (1) *X.509-Zertifikate für VAU-Verbindungen und X.509-Zertifikate für SGD-Verbindungen*[558] (2) *öffentlicher ECIES-Schlüssel eines SGD-HSMs* when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/ **SGDVAU**	The TSF shall use *the following rules* *(1) Für X.509-Zertifikate für VAU-Verbindungen und X.509-Zertifikate für SGD-Verbindungen müssen die „interpretation rules“ nach FPT_TDC.1/NK.TLS.Zert umgesetzt werden.* *(2) Das VAU Zertifikat muss die OID oid_epa_vau ([50]) haben.* *(3) Das SGD Zertifikat muss die OID oid_SGD{1/2}_hsm (siehe A_17848 und [50]) und die korrekte Servicetypkennung („http://uri.etsi.org/TrstSvc/Svctype/unspecified“, siehe A_17847) haben.* [559] *(4) Der öffentliche ECIES-Schlüssel eines SGD-HSMs muss die Kodierung nach A_17894-01 aufweisen.* when interpreting the TSF data from another trusted IT product.

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

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

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

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

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

6.4. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

Es wird die Vertrauenswürdigkeitsstufe **EAL3** erweitert um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2 gefordert. Daraus ergibt sich eine **Resistenz gegen „Enhanced Basic“ Angriffspotential**. Eine Erklärung für die gewählte EAL-Stufe findet sich in Abschnitt 6.5.7.

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

6.4.1. Verfeinerungen entsprechend Schutzprofil

6.4.1.1. Verfeinerung zur Vertrauenswürdigkeitskomponente ADV_ARC.1

In Hinblick auf den EVG-Teil Netzkonnektor gilt die folgende Verfeinerung:

> **Die Sicherheitsarchitektur muss beschreiben, wie der EVG Daten, Kommunikationspfade und Zugriffe der unterschiedlichen Dienste und Anwendungen separiert.**
>
> **Der Hersteller muss die Sicherheitsarchitektur beschreiben. Die Beschreibung der Sicherheitsarchitektur muss zeigen, auf welche Weise die Sicherheitsarchitektur des EVGs die Separation der unterschiedlichen Dienste und Anwendungen (zwischen LAN und WAN sowie zwischen den Updatemechanismen und dem Datenfluss im Normalbetrieb) sicherstellt.**
>
> **Der Evaluator muss die Beschreibung analysieren (examine), um festzustellen, dass sie beschreibt, auf welche Weise die Sicherheitsarchitektur des EVGs die Separation der unterschiedlichen Dienste und Anwendungen sicherstellt.**

In Hinblick auf den EVG-Teil Anwendungskonnektor gilt die folgende Verfeinerung:

> Das Element ADV_ARC.1.4C wird durch den Zusatz verfeinert:
>
> **Die Sicherheitsarchitekturbeschreibung muss den Selbstschutz**
>
> **(1) vor Missbrauch der TSF durch Verwendung des EVT_MONITOR_OPERATIONS [27],**
> **(2) der Vertraulichkeit und der Integrität der TSF-Daten (s. TIP1-A_4813 Persistieren der Konfigurationsdaten [27]),**
> **(3) vor Entnahme der gSMC-K und Kompromittierung der Kommunikation der gSMC-K mit dem EVG**
>
> **beschreiben.**

6.4.1.2. Verfeinerung zur Vertrauenswürdigkeitskomponente Betriebsdokumentation AGD_OPE.1 zu Signaturrichtlinien

In Hinblick auf den EVG-Teil Netzkonnektor gilt die folgende Verfeinerung:

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

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

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

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

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

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

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

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

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

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

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

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

In Hinblick auf den EVG-Teil Anwendungskonnektor gilt die folgende Verfeinerung:

Das Element AGD_OPE.1.1C wird durch den Zusatz verfeinert:

Die Benutzerdokumentation muss alle im EVG implementierten Signaturrichtlinien und Verschlüsselungsrichtlinien beschreiben und Informationen zu deren Anwendung bereitstellen. Für jede implementierte Signaturrichtlinie muss die Benutzerdokumentation beschreiben:

- **den Namen der Signaturrichtlinie**
- **die Signaturart, d. h. qualifizierte elektronische Signatur, fortgeschrittene oder digitale Signatur,**
- **die gemäß dieser Signaturrichtlinie signierten Daten.**

Für jede implementierte Verschlüsselungsrichtlinie muss die Benutzerdokumentation beschreiben:

- **den Namen der Verschlüsselungsrichtlinie**
- **die gemäß dieser Verschlüsselungsrichtlinie verschlüsselten Daten.**
- **die unter dieser Verschlüsselungsrichtlinie erlaubten Empfänger der Daten.**

6.4.1.3. Verfeinerung zur Vertrauenswürdigkeitskomponente Betriebsdokumentation AGD_PRE.1

In Hinblick auf den EVG-Teil Anwendungskonnektor gilt die folgende Verfeinerung:

Das Element AGD_PRE.1.1C wird durch den Zusatz verfeinert:
Der Hersteller muss beschreiben, auf welche Weise das Verfahren zur Inbetriebnahme (in Verbindung mit dem Auslieferungsverfahren gemäß ALC_DEL.1.1C) sicherstellt, dass nur authentische EVGs in Umlauf gebracht werden können.

Das Element AGD_PRE.1.2C wird durch den Zusatz verfeinert:

Der Hersteller muss die Installation von Updates gemäß [27], Kapitel 4.3.9, und das Verfahren zur Inbetriebnahme von Updates des EVGs in der Benutzerdokumentation beschreiben.

Das Element AGD_PRE.1.1E wird durch den Zusatz verfeinert:

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

6.4.1.4. Verfeinerung von ALC_DEL.1

Für den EVG gilt die folgende Verfeinerung:

ALC_DEL.1 wird wie folgt verfeinert:

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

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

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

6.4.2. Verfeinerungen hinsichtlich der Fachmodule NFDM, AMTS und ePA

Im folgenden sind zusärtzliche Prüfanforderungen an die Fachmodule des Konnektors formuliert. Siehe dazu auch die „Erweiterungen für unterstützte Fachmodule“ in Kapitel 8.2.

Das Fachmodul VSDM ist integraler Bestandteil des Anwendungskonnektors und wurde vollständig in den Sicherheitsanforderungen des zugrundeleigenenden Schutzprofils und dieser Sicherheitsvorgaben berücksichtigt.

Der secunet konnektor 2.0.0 enthält in seiner Ausbaustufe PTV5 WR1 neben dem VSDM Fachmodul die modular integrierten Fachmodule ePA (nach [49]), NFDM (nach [44]) und AMTS (nach [45]).

Entsprechend der Technischen Richtlinien TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 sollen

> *...für das Fachmodul relevante Sicherheitseigenschaften des Konnektors zusätzlich in dessen Security Target aufgenommen und Common Criteria-zertifiziert werden, wenn diese im [PP0098] nicht enthalten sind.*

In der TR-03157 ([26]), Kapitel 3.2.2, wird entsprechend gefordert:

> *Die Anforderungen aus dem Produkttypsteckbrief müssen daher zusätzlich zum PP im Konnektor-ST aufgenommen und mitzertifiziert werden.*

und

> *Schnittstellen die eine Sicherheitsleistung für das Fachmodul erbringen, müssen im Rahmen der CC-Zertifizierung mit geprüft werden.*

Die jeweils relevanten Sicherheitseigenschaften sowie die vom jeweiligen Fachmodul aufgerufene TUCs nach [27] werden in Kapitel 3.3.2 bzw. 3.2.2 der Technischen Richtlinien aufgeführt. Um sicherzustellen, dass im Rahmen der Evaluierung nach Common Criteria diese Sicherheitseigenschaften hinreichend berücksichtigt werden, sind die folgenden Anforderungen an die Vertrauenswürdigkeit (Assurance) entsprechend verfeinert:

Für den EVG gelten die folgende Verfeinerungen:

> ASE_TSS.1 wird wie folgt verfeinert:
>
> **Der Konnektor unterstützt die Fachmodule ePA, NFDM und AMTS. In den Technischen Richtlinien TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 bzw. TR-03157 ([26]), Kapitel 3.2.2, werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die für die Fachmodule ePA, NFDM und AMTS relevanten Sicherheitseigenschaften des Konnektors müssen zusätzlich im Security Target des Konnektors aufgenommen werden.**
>
> **Der Hersteller muss im Security Target beschreiben, dass der Konnektor die nach TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 bzw. TR-03157 ([26]), Kapitel 3.2.2, relevanten Sicherheitseigenschaften des Konnektors umsetzt.**
>
> **Der Evaluator muss prüfen, ob die nach TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 bzw. TR-03157 ([26]), Kapitel 3.2.2, relevanten Sicherheitseigenschaften des Konnektors vollständig im Security Target berücksichtigt sind.**
>
> ADV_FSP.4 wird wie folgt verfeinert:
>
> **Der Konnektor unterstützt die Fachmodule ePA, NFDM und AMTS. In den Technischen Richtlinien TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 bzw. TR-03157 ([26]), Kapitel 3.2.2, werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die dabei von**

den Fachmodulen aufgerufenen Schnittstellen des Anwendungskonnektors müssen beschrieben werden.

Der Hersteller muss eine Beschreibung der Schnittstellen des Anwendungskonnektors bereitstellen, an denen die relevanten Sicherheitseigenschaften des Konnektors umgesetzt werden.

Der Evaluator muss die Beschreibung der Schnittstellen des Anwendungskonnektors, an denen die relevanten Sicherheitseigenschaften des Konnektors umgesetzt werden auf Vollständigkeit hinsichtlich der Vorgaben in den Technischen Richtlinien prüfen.

Die Prüfung der sicheren und korrekten Implementierung der von den Schnittstellen bereitgestellten relevanten Sicherheitseigenschaften des Konnektors wird durch die Verfeinerung von ADV_TDS gefordert.

ADV_TDS.3 wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule ePA, NFDM und AMTS. In den Technischen Richtlinien TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 bzw. TR-03157 ([26]), Kapitel 3.2.2, werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften muss geprüft werden.

Der Hersteller muss ausreichende Nachweise bereitstellen, die es erlauben die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften zu prüfen.

Der Evaluator muss die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften prüfen.

Die Nachweise des Herstellers können zum Beispiel eine Beschreibung der von den Fachmodulen aufgerufenen Schnittstellen und die Abbildung der relevanten TUCs auf den Source Code enthalten. Im Rahmen der Evaluierung kann auch auf andere Prüfaspekte, wie zum Beispiel ADV_FSP, ADV_IMP oder ATE verwiesen werden, wenn darin entsprechende Prüfnachweise erbracht wurden.

6.5. Erklärung der Sicherheitsanforderungen

6.5.1. Erklärung der Abhängigkeiten der funktionalen Sicherheitsanforderungen des Netzkonnektors

Die Abhängigkeiten für die SFRs des Netzkonnektors sind bei deren Formulierung in Abschnitt 6.2 aufgelöst.

6.5.2. Erklärung der Abhängigkeiten der funktionalen Sicherheitsanforderungen des Anwendungskonnektors

Die Abhängigkeiten für die SFRs des Anwendungskonnektors werden im Schutzprofil [16], Tabelle 25, aufgelöst und gelten unverändert auch für diese Sicherheitsvorgaben. Es wurden keine SFRs des Anwednungskonnekors aus [16] in diesen Sicherheitsvorgaben weggelassen oder darüber hinaus hinzugefügt.

Die Abhängigkeiten für die zusätzlichen SFRs der ePA Fachanwendung in Abschnitt 6.3.7 sind bei deren Formulierung aufgelöst

6.5.3. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors durch SFRs des Netzkonnektors

Tabelle 27 stellt die Abbildung der Sicherheitsziele des Netzkonnektors auf Sicherheitsanforderungen des Netzkonnektors zunächst tabellarisch im Überblick dar. In Abschnitt 6.5.5 wird die Abbildung erläutert und die Erfüllung der Sicherheitsziele durch die Anforderungen begründet.

Sicherheitsanforderung an den EVG	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.Admin_Auth	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FTP_ITC.1/NK.VPN_TI									X		X	X			
FTP_ITC.1/NK.VPN_SIS									X		X	X			
FDP_IFC.1/NK.PF													X	X	X
FDP_IFF.1/NK.PF													X	X	X
FMT_MSA.3/NK.PF													X	X	
FPT_STM.1/NK					X	X									
FPT_TDC.1/NK.Zert										X					
FDP_RIP.1/NK		X													
FPT_TST.1/NK		X													
FPT_EMS.1/NK		X									X	X			
FAU_GEN.1/NK.SecLog					X										
FAU_GEN.2/NK.SecLog					X										
FMT_SMR.1./NK	X			X									X	X	

Sicherheitsanforderung an den EVG	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.Admin_Auth	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FMT_MTD.1/NK				X											
FIA_UID.1/NK.SMR				X											
FIA_UAU.1/NK.SMR				X				X							
FTP_TRP.1/NK.Admin	X			X				X							
FMT_SMF.1/NK	X			X									X	X	
FMT_MSA.1/NK.PF				X									X	X	
FCS_COP.1/NK.Hash		X										X			
FCS_COP.1/NK.HMAC												X			
FCS_COP.1/NK.Auth			X						X						
FCS_COP.1/NK.ESP											X				
FCS_COP.1/NK.IPsec											X				
FCS_CKM.1/NK		X	X						X		X	X			
FCS_CKM.2/NK.IKE									X		X	X			
FCS_CKM.4/NK	X	X	X						X		X	X			
FTP_ITC.1/NK.TLS	X							X							
FPT_TDC.1/NK.TLS.Zert	X														
FCS_CKM.1/NK.TLS	X														
FCS_COP.1/NK.TLS.HMAC	X														
FCS_COP.1/NK.TLS.AES	X														
FCS_COP.1/NK.TLS.Auth	X														
FCS_CKM.1/NK.Zert	X														
FDP_ITC.2/NK.TLS	X														
FDP_ETC.2/NK.TLS	X														
FMT_MOF.1/NK.TLS	X														
FDP_ACC.1/NK.Update							X								
FDP_ACF.1/NK.Update							X								
FDP_ITC.1/NK.Update							X								
FDP_UIT.1/NK.Update							X								

Tabelle 27: Abbildung der EVG-Ziele auf Sicherheitsanforderungen

6.5.4. Überblick der Abdeckung von Sicherheitszielen des Konnektors durch SFRs des Netzkonnektors und des Anwendungskonnektors

Funktionale Sicherheits-anforderung (SFR)	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FCS_CKM.1/NK.TLS	X		X																X									
FCS_COP.1/NK.TLS.HMAC	X		X																X	X								
FCS_COP.1/NK.TLS.AES	X		X																X	X								
FCS_COP.1/NK.TLS.Auth	X		X																X	X								
FCS_CKM.1/NK.Zert																			X									
FDP_ETC.2/NK.TLS																			X									
FDP_ITC.2/NK.TLS																			X									
FTP_TRP.1/NK.Admin																							X					
FAU_GEN.1/AK		X																			X							
FAU_SAR.1/AK		X																			X							
FAU_STG.1/AK		X																			X							
FAU_STG.4/AK		X																			X							
FCS_CKM.1/AK.AES	X		X				X																					
FCS_CKM.4/AK	X		X				X	X																				
FCS_COP.1/AK.AES	X						X	X																				
FCS_COP.1/AK.CMS.Ent	X							X																				
FCS_COP.1/AK.CMS.SigPr	X																X											
FCS_COP.1/AK.CMS.Sign	X									X	X																	
FCS_COP.1/AK.CMS.Ver	X						X																					
FCS_COP.1/AK.PDF.SigPr	X																X											
FCS_COP.1/AK.PDF.Sign	X									X	X																	
FCS_COP.1/AK.SigVer.ECDSA																	X											
FCS_COP.1/AK.SigVer.PSS	X														X		X											
FCS_COP.1/AK.SigVer.SSA	X														X		X											
FCS_COP.1/AK.SHA	X									X	X				X		X											
FCS_COP.1/AK.XML.Ent	X							X																				
FCS_COP.1/AK.XML.Sign	X									X																		
FCS_COP.1/AK.XML.SigPr	X																X											
FCS_COP.1/AK.XML.Ver	X						X																					
FDP_ACC.1/AK.eHKT			X																									

Funktionale Sicherheits-anforderung (SFR)	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FDP_ACC.1/AK.Enc							X	X																				
FDP_ACC.1/AK.Infomod																								X		X		
FDP_ACC.1/AK.KD				X																								
FDP_ACC.1/AK.PIN				X		X																			X			
FDP_ACC.1/AK.Sgen									X	X	X	X	X	X														
FDP_ACC.1/AK.SigPr															X	X	X											
FDP_ACC.1/AK.TLS																			X	X							X	X
FDP_ACC.1/AK.SDS		X																										
FDP_ACC.1/AK.Update																							X					
FDP_ACC.1/AK.VSDM																											X	
FDP_ACF.1/AK.eHKT			X																									
FDP_ACF.1/AK.Enc							X	X																				
FDP_ACF.1/AK.Infomod																								X		X		
FDP_ACF.1/AK.KD				X																				X				
FDP_ACF.1/AK.PIN				X		X																			X			
FDP_ACF.1/AK.Sgen									X	X	X	X	X	X														
FDP_ACF.1/AK.SigPr															X	X	X											
FDP_ACF.1/AK.TLS																			X	X							X	X
FDP_ACF.1/AK.SDS		X																										
FDP_ACF.1/AK.Update																							X					
FDP_ACF.1/AK.VSDM																											X	
FDP_DAU.2/AK.Cert										X					X	X	X											
FDP_DAU.2/AK.QES										X					X	X	X											
FDP_DAU.2/AK.Sig											X				X	X	X											
FDP_ETC.2/AK.Enc							X	X																				
FDP_ITC.2/AK.Enc							X	X																				
FDP_ITC.2/AK.Sig										X																		
FDP_RIP.1/AK			X		X		X	X	X																			
FDP_SDI.2/AK									X																			
FDP_UCT.1/AK.TLS			X																									
FDP_UIT.1/AK.TLS			X																									
FDP_UIT.1/AK.Update																							X					
FIA_API.1/AK													X	X														
FIA_SOS.1/AK.Passwörter		X								X																		

Funktionale Sicherheits-anforderung (SFR)	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FIA_SOS.2/AK.Jobnummer						X			X																			
FIA_SOS.2/AK.PairG			X																									
FIA_UAU.1/AK		X					X	X							X	X	X											
FIA_UAU.5/AK		X	X	X		X				X		X	X	X														
FIA_UID.1/AK					X																							
FMT_MSA.1/AK.User									X																			
FMT_MSA.1/AK.Infomod																										X		
FMT_MSA.3/AK.Infomod																										X		
FMT_MSA.1/AK.TLS		X																	X	X							X	X
FMT_MSA.3/AK.TLS		X																	X	X							X	X
FMT_MSA.1/AK.VSDM																											X	
FMT_MSA.3/AK.VSDM																											X	
FMT_MSA.3/AK.Sig										X					X													
FMT_MSA.4/AK									X				X	X														
FMT_MOF.1/AK		X																										
FMT_MTD.1/AK.Admin		X	X	X		X																						
FMT_MTD.1/AK.Zert		X		X																								
FMT_MTD.1/AK.eHKT_Abf		X	X																									
FMT_MTD.1/AK.eHKT_Mod		X	X																									
FMT_SMF.1/AK		X	X	X		X			X																			
FMT_SMR.1/AK		X	X	X		X			X																			
FPT_FLS.1/AK					X													X			X					X		
FPT_STM.1/AK																						X						
FPT_TDC.1/AK			X	X			X			X					X	X							X					
FPT_TEE.1/AK			X	X		X																						
FPT_TST.1/AK.Out-Of-Band					X													X										
FPT_TST.1/AK.Run-Time					X													X										
FTA_TAB.1/AK.Jobnummer						X			X																			
FTA_TAB.1/AK.SP													X	X														
FTP_ITC.1/AK.CS																			X									
FTP_ITC.1/AK.eHKT			X																									

Funktionale Sicherheits-anforderung (SFR)	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FTP_ITC.1/AK.FD																				X							X	
FTP_ITC.1/AK.QSEE									X				X	X														
FTP_ITC.1/AK.VZD																												X
FTP_ITC.1/AK.KSR																							X					
FTP_ITC.1/AK.TSL																							X					

Tabelle 28: Abdeckung der Sicherheitsziele des EVG durch Sicherheitsanforderungen

Sicherheitsanforderung an den EVG	O.AK.VAUSGD (Anteil VAU)	O.AK.VAUSGD (Anteil SGD)
FTP_ITC.1/VAU	X	
FCS_CKM.1/VAU	X	
FCS_COP.1/VAU.AES	X	
FCS_COP.1/VAU.Auth	X	
FTP_ITC.1/SGD		X
FCS_COP.1/SGD.ECIES		X
FCS_COP.1/SGD.Auth		X
FDP_ITC.2/SGD		X
FDP_ACC.1/SGD		X
FDP_ACF.1/SGD		X
FPT_TDC.1/SGDVAU	X	X
FCS_CKM.4/AK	X	X

Tabelle 29: Abdeckung der Sicherheitsziele der ePA Fachanwendung durch Sicherheitsanforderungen

6.5.5. Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors

In diesem Abschnitt wird erklärt, warum die Kombination der individuellen funktionalen Sicherheitsanforderungen (SFR) und Anforderungen an die Vertrauenswürdigkeit (SAR) für den EVG gemeinsam die formulierten Sicherheitsziele erfüllen.

Dazu wird in der folgenden Tabelle 30 jedes EVG-Ziel in einzelne Teilaspekte zerlegt, die dann auf Sicherheitsanforderungen abgebildet werden.[560] Um die Abbildung zu erklären (im Sinne des von Common Criteria geforderten Erklärungsteils / Rationale), wird in der Tabelle zu jeder solchen Abbildung eines Aspekts in der folgenden Zeile eine Begründung gegeben. Die Begründung zitiert, wo dies möglich ist, Sätze aus dem entsprechenden EVG-Ziel. Solche Zitate sind durch Anführungszeichen und Kursivschrift gekennzeichnet.

Grundsätzlich gilt, dass die korrekte Umsetzung eines Ziel in Sicherheitsanforderungen durch die im CC Teil 2 [5] aufgeführten Abhängigkeiten zwischen funktionalen Sicherheitsanforderungen (SFRs) unterstützt wird: Häufig lässt sich leicht ein SFR finden, welches wesentliche Aspekte des EVG-Ziels umsetzt. Betrachtet man alle Abhängigkeiten, so ergibt sich eine vollständige Abdeckung des EVG-Ziels. In der folgenden Tabelle werden daher abhängige SFRs ebenfalls mit aufgelistet. Dabei wird davon ausgegangen, dass die Abhängigkeit selbst nicht gesondert erläutert werden muss.

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
O.NK.TLS_**Krypto**	TLS-Kanäle	FTP_ITC.1/NK.TLS FMT_MOF.1/NK.TLS FMT_SMR.1./NK FMT_SMF.1/NK FPT_TDC.1/NK.TLS.Zert
	Begründung: In O.NK.TLS_**Krypto** wird gefordert: *„Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung“* Genau dies leistet FTP_ITC.1/NK.TLS. Mit FMT_MOF.1/NK.TLS wird der Rolle Anwendungskonnektor die Möglichkeit gegeben die TLS-Verbindungen zu Managen und je nach Anwendungsfall einzurichten. FMT_SMF.1/NK definiert diese Funktionalität und FMT_SMR.1./NK definiert diese Rolle (Anwendungskonnektor). Zertifikate die im Rahmen von TLS-Verbindungen zum Einsatz kommen werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.	
	Kommunikation mit anderen IT-Produkten	FCS_CKM.1/NK.Zert FCS_CKM.4/NK FDP_ITC.2/NK.TLS

[560] Hinweis: Common Criteria fordert nur eine Abbildung der EVG-Ziele auf funktionale Sicherheitsanforderungen (SFRs). Es zeigte sich aber, dass auch Anforderungen an die Vertrauenswürdigkeit (SARs) bzw. deren Verfeinerungen einen Beitrag zum Erreichen der Sicherheitsziele leisten

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Gültigkeitsprüfung von Zertifikaten	FTP_TRP.1/NK.Admin FDP_ETC.2/NK.TLS FPT_TDC.1/NK.TLS.Zert
	Begründung: Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der EVG das exportieren von X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle (FDP_ETC.2/NK.TLS). Entsprechende Zertifikate können vom EVG durch die in FCS_CKM.1/NK.Zert geforderten Mechanismen erzeugt werden, FCS_CKM.4/NK unterstützt als abhängige Komponente. Zertifikate für Clientsysteme können auch vom EVG gemäß FDP_ITC.2/NK.TLS über die gesicherte Management-Schnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Die importierten Zertifikate werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert. Dabei wird auch eine Gültigkeitsprüfung der Zertifikate durchgeführt.	
	sichere kryptographische Algorithmen und Protokolle	FCS_CKM.1/NK.TLS FCS_COP.1/NK.TLS.HMAC FCS_COP.1/NK.TLS.AES FCS_COP.1/NK.TLS.Auth FCS_CKM.4/NK
	Begründung: Für die TLS-Kanäle sind nach O.NK.TLS_**Krypto** nur „*sichere kryptographische Algorithmen und Protokolle gemäß [19] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [30]*“ zugelassen. FCS_COP.1/NK.TLS.Auth die unterstützt die Authentisierung im Rahmen des TLS-Verbindungsaufbaus, indem der dazu zu verwendende Algorithmus spezifiziert wird. FCS_COP.1/NK.TLS.HMAC spezifiziert die HMAC Algorithmen, die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen. Nach erfolgreichem Verbindungsaufbau wird die Kommunikation mit AES gemäß FCS_COP.1/NK.TLS.AES abgesichert. FCS_CKM.1/NK.TLS fordert, dass entsprechendes Schlüsselmaterial generiert wird, FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Schutz	Speicheraufbereitung: temporäre Kopien nicht mehr benötigter Geheimnisse werden unmittelbar nach Gebrauch aktiv überschrieben	FDP_RIP.1/NK

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Begründung: In **O.NK.Schutz** wird gefordert: „*Der EVG löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden.*“ Genau dies leistet FDP_RIP.1/NK. Auch die Zuweisung „upon the *deallocation of the resource from*“ passt zur Forderung in **O.NK.Schutz**. Die „*Geheimnisse (z. B. Schlüssel)*“ werden im SFR durch die Zuweisung präzisiert.	
	Selbsttests, Schutz gegen sicherheitstechnische Veränderungen	FPT_TST.1/NK
	Begründung: „*Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten:*“ → ist als Erläuterung für die Begriffsbildung **O.NK.Schutz**und als Oberbegriff für die weiteren Teilaspekte zu verstehen. „*Der EVG schützt sich selbst gegen sicherheitstechnische Veränderungen an den äußeren logischen Schnittstellen bzw. erkennt diese oder macht diese erkennbar. Der EVG erkennt bereits Versuche, sicherheitstechnische Veränderungen durchzuführen, sofern diese über die äußeren Schnittstellen des EVGs erfolgen (mit den unter OE.NK.phys_Schutz formulierten Einschränkungen). Der EVG führt beim Start-up und bei Bedarf Selbsttests durch.*“ → Das Erkennen bzw. Erkennbarmachen sicherheitstechnischer Veränderungen erfolgt durch den von FPT_TST.1/NK geforderten Selbsttest. Im Rahmen der Integritätsprüfungen werden Hashwerte wie von FCS_COP.1/NK.Hash gefordert verwendet. Dieses SFR hat die formalen Abhängigkeiten FCS_CKM.4/NK und FCS_CKM.1/NK, wobei FCS_CKM.4/NK nicht erfüllt werden muss, sofern im Rahmen der Hashwertberechnung keine geheimen Schlüssel verwendet werden. FCS_CKM.1/NK fordert, dass das Schlüsselmaterial (z. B. Integritätsprüfschlüssel) generiert wird. Anmerkung: Alternativ könnte ein Hersteller diese Schlüssel auch importieren; dazu wäre dann zusätzlich FDP_ITC.1 oder FDP_ITC.2 aufzunehmen.	
	Schutz gegen unbefugte Kenntnisnahme (Side Channel-Analysen)	FPT_EMS.1/NK
	Begründung: „*Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten.*“ Um den Aspekt „*die ihm anvertrauten Benutzerdaten*“ vollständig abzudecken, wurde die explizite Komponente FPT_EMS.1/NK	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	ergänzt. Dieses SFR fordert genau die Analyse, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen.	
O.NK.Stateful	dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	FDP_IFC.1/NK.PF → FDP_IFF.1/NK.PF
	Begründung: „*Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter.*“ Diese Paketfilterung wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF). Die zustandsgesteuerte Filterung wurde in den Operationen und im Refinement zu FDP_IFF.1/NK.PF modelliert.	
O.NK.EVG_Authenticity	Auslieferungsverfahren: Nur authentische EVGs können in Umlauf gebracht werden	FCS_COP.1/NK.Auth FCS_CKM.1/NK FCS_CKM.4/NK
	Begründung: „*Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können. Gefälschte EVGs müssen vom VPN-Konzentrator sicher erkannt werden können. Der EVG muss auf Anforderung mit Unterstützung der SM NK einen Nachweis seiner Authentizität ermöglichen.*“ → Die Authentisierung wird mit Kryptoalgorithmen erbracht, die durch FCS_COP.1/NK.Auth spezifiziert werden. FCS_CKM.1/NK fordert eine Generierung des für den Nachweis der Authentizität des EVGs erforderlichen Schlüsselmaterials; FCS_CKM.4/NK unterstützt als abhängige Komponenten dabei.	
O.NK.Admin_EVG	rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen Identifikation / Autorisierung des Administrators sicherer Pfad Beschränkung der Administration der Firewall-Regeln	FMT_MTD.1/NK FMT_SMR.1./NK FMT_SMF.1/NK FIA_UID.1/NK.SMR FIA_UAU.1/NK.SMR FTP_TRP.1/NK.Admin FMT_MSA.1/NK.PF
	Begründung: „*Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen.*“ → FMT_MTD.1/NK beschränkt den Zugriff wie vom Ziel gefordert auf die Rolle Administrator. FMT_SMR.1./NK modelliert als abhängige	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Komponente diese Rolle (Administrator). FIA_UID.1/NK.SMR erfordert eine Identifikation des Benutzers vor jeglichem Zugriff auf administrative Funktionalität. Die Menge der administrativen Funktionen wird in FMT_SMF.1/NK aufgelistet. „*Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung eines Administrators, welcher die lokale und entfernte Administration des EVG durchführen kann.*“ → Die Authentisierung des Administrators erfolgt durch den EVG. Die dabei anzuwendenden Regeln wurden in FIA_UAU.1/NK.SMR modelliert. „*Die Administration erfolgt rollenbasiert.*“ → FMT_SMR.1./NK modelliert die Rolle Administrator. „*Weil die Administration über Netzverbindungen (lokal über PS2 oder zentral über PS3) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).*“ → FTP_TRP.1/NK.Admin fordert genau diesen sicheren logischen Kanal zum Benutzer (trusted path). „*Der EVG verhindert die Administration folgender Firewall-Regeln: …*“ → Dieser Aspekt wird durch das Refinement zu FMT_MSA.1/NK.PF abgebildet. Schließlich unterstützt die Benutzerdokumentation (AGD_OPE.1) bei der Administration der Paketfilter-Regeln.	
O.NK.Protokoll	EVG protokolliert sicherheitsrelevante Ereignisse mit Daten und Zeitstempel	FAU_GEN.1/NK.SecLog FAU_GEN.2/NK.SecLog FPT_STM.1/NK
	Begründung: „*Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit.“* → FAU_GEN.1/NK.SecLog fordert eine Protokollierung für die in der Operation explizit aufgelisteten Ereignisse und stellt Anforderungen an den Inhalt der einzelnen Log-Einträge. FAU_GEN.2/NK.SecLog fordert, dass die Benutzeridentitäten mit protokolliert werden. FPT_STM.1/NK stellt den Zeitstempel bereit.	
O.NK.Zeitdienst	regelmäßige Zeitsynchronisation	FPT_STM.1/NK
	Begründung: „*Der EVG synchronisiert die Echtzeituhr gemäß OE.NK*.Echtzeituhr *in regelmäßigen Abständen über einen sicheren Kanal mit einem vertrauenswürdigen Zeitdienst (siehe OE.NK*.Zeitsynchro*).*“ → (Refinement zu) FPT_STM.1/NK: Synchronisation mindestens einmal innerhalb von 24 Stunden; Information, falls die Synchronisierung nicht erfolgreich durchgeführt werden konnte	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
O.NK.Update	Software Update	FDP_ACC.1/NK.Update FDP_ACC.1/NK.Update FDP_ITC.1/NK.Update FDP_UIT.1/NK.Update
	Begründung: Das Sicherheitsziel O.NK.Update „Software Update“ fordert vom EVG die Aktualisierung von Software-Komponenten sowie deren Prüfung auf Integrität. FDP_ACC.1/NK.Update führt die Update-SFP für den Software-Update ein und FDP_ACC.1/NK.Update definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_ITC.1/NK.Update fordert die Fähigkeit des EVG zum Import der Software-Komponenten von ausserhalb des EVG und FDP_UIT.1/NK.Update fordert die Prüfung der Integrität dieser Daten vor dem Update.	
O.NK.Admin_Auth	Authentisierung des Administrators	FTP_TRP.1/NK.Admin FIA_UAU.1/NK.SMR FTP_ITC.1/NK.TLS
	Begründung: FTP_TRP.1/NK.Admin fordert einen sicheren Kommunikationskanal zwischen EVG und Administrator. FTP_ITC.1/NK.TLS fordert dazu einen TLS-Kanal für lokale und entfernte Administrierung. Erst nach erfolgreicher Authentisierung können adminstrative Funktionen aufgerufen werden (FIA_UAU.1/NK.SMR).	
O.NK.VPN_Auth	gegenseitige Authentisierung mit VPN-Konzentrator (Telematikinfrastruktur-Netz)	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Auth → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK
	Begründung: FCS_COP.1/NK.Auth setzt direkt die Anforderung nach einer Authentisierung des EVGs gegenüber dem VPN-Konzentrator um, indem es die dazu zu verwendenden Algorithmen spezifiziert. FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS fordern die sicheren Kanäle mit gegenseitiger Authentifizierung („ … provides assured identification of its end points …“) zu den VPN-Konzentratoren in die Telematikinfrastruktur bzw. ins Internet. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS (IPsec) und FCS_CKM.2/NK.IKE (IKE) legen fest, welche Protokolle im Rahmen des Kanalaufbaus verwendet werden sollen. Zwar geht es in	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	FCS_CKM.2/NK.IKE vorrangig um die Schlüsselableitung, diese ist aber mit der Authentisierung kombiniert. FCS_CKM.1/NK fordert, dass entsprechendes Schlüsselmaterial für die Authentisierung generiert wird (evtl. unter Rückgriff auf eine gSMC-K, welches in den EVG eingebracht wird). FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Zert_Prüf	Gültigkeitsprüfung von Zertifikaten mit Hilfe von TSL und der CRL	FPT_TDC.1/NK.Zert
	Begründung: Zertifikatsprüfung: „*Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form einer zugehörigen **CRL** und einer **TSL** bereitgestellt.*“ FPT_TDC.1/NK.Zert fordert, dass der EVG Informationen über die Gültigkeit von Zertifikaten korrekt interpretiert. In der Zuweisung wurden **TSL** und CRL explizit erwähnt: „*The TSF shall provide the capability to consistently interpret information – distributed in the form of a **TSL (Trust-Service Status List)** or **CRL (Certificate Revocation List)** information …*“ Die Zertifikatsprüfung wird für VPN-Konzentratoren der Telematikinfrastruktur-Netzes bzw. des Sicheren Internet Service durchgeführt. FPT_TDC.1/NK.Zert fordert ferner explizit, dass der EVG Informationen „*about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects”* interpretiert.	
O.NK.VPN_Vertraul	Vertraulichkeit der Nutzdaten im VPN (Telematikinfrastruktur-Netz) IPsec-Kanal: Ableitung von *session keys*, AES-Verschlüsselung mit den *session keys* , Zerstörung der *session keys* nach Verwendung, Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.IPsec, → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_COP.1/NK.ESP → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Vertraulichkeit der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Konzentratoren verschlüsselt (vor dem Versand) bzw. entschlüsselt (nach dem Empfang) der Konnektor die Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Verschlüsselung wird durch FTP_ITC.1/NK.VPN_TI (im Fall der Telematikinfrastruktur) bzw. FTP_ITC.1/NK.VPN_SIS (im Fall des Sicheren Internet Service) gefordert *(„ …protection of the channel data from modification and disclosure“*, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.IPsec ermöglicht die Definition der zu verwendenden Verschlüsselungsalgorithmen, hier AES gemäß FCS_COP.1/NK.ESP. FCS_CKM.4/NK unterstützt als abhängige Komponente ebenfalls. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet. FCS_CKM.1/NK fordert eine solche Generierung von *session keys*. *„ Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.“* → Mittels FCS_CKM.2/NK.IKE (IKE) werden die abgeleiteten Sitzungsschlüssel, die für die Verschlüsselung verwendet werden, mit der die Vertraulichkeit der Nutzdaten sichergestellt wird, mit der Gegenstelle ausgetauscht. Die Nutzdaten werden mit AES gemäß FCS_COP.1/NK.ESP verschlüsselt. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.VPN_Integrität	Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von *session keys*, Austausch der *session keys* mit Gegenstelle, Zerstörung der *session keys* nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von *session keys*, Zerstörung der *session keys* nach Verwendung Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Hash → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK FCS_COP.1/NK.HMAC → FCS_CKM.1/NK → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Integritätssicherung wird durch FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS gefordert („*...protection of the channel data from modification and disclosure*“, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Encapsulating Security Payload (ESP) (RFC 4303 (ESP), [59]) erfolgt. erfolgt, wobei die Authentizitätsdaten (authentication data) den Wert des Integritätstests (integrity check value) enthalten, der sich wiederum aus einem Hash über den ESP Header und den verschlüsselten Nutzdaten des Paketes ergibt. Insofern ist eine Hashfunktion erforderlich. Weiterhin ist im IPSec sowie in IKE Standard die Verwendung von HMAC Algorithmen enthalten ([62], [63], [60]). Dies wird durch FCS_COP.1/NK.HMAC erreicht. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet (FCS_CKM.1/NK) und mit der Gegenstelle ausgetauscht (FCS_CKM.2/NK.IKE). FCS_CKM.4/NK unterstützt als abhängige Komponente. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.PF_WAN	dynamischer Paketfilter zum WAN	FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, FMT_MSA.3/NK.PF, FMT_MSA.1/NK.PF, FMT_SMR.1./NK FMT_SMF.1/NK AVA_VAN.5 (hohes Angriffspotential)
	Begründung: „*Der EVG schützt sich selbst, andere Konnektorteile und die Clientsysteme vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN).“* → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „*The TSF*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	shall enforce the packet filtering SFP (PF SFP) on the subjects VPN concentrator and attacker communicating with the TOE from its WAN interface (PS3) …“ FDP_IFF.1/NK.PF modelliert einen Paketfilter („*…the decision shall be based on the following security attributes: IP address, port number, and protocol type.*“, „*For every operation (…) the TOE shall maintain a set of packet filtering rules …*“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (*Stateful Packet Inspection*) abgebildet und durch ein Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF (für die Paketfilterregeln im Allgemeinen). Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen (z. B Administrator) und verhindert so unbefugte Veränderungen an den sicherheitsrelevanten Filterregeln. FMT_SMR.1./NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf.	
O.NK.PF_LAN	dynamischer Paketfilter zum LAN, regelbasierte Informationsflusskontrolle	FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, FMT_MSA.3/NK.PF, FMT_MSA.1/NK.PF, FMT_SMR.1./NK FMT_SMF.1/NK FDP_IFF.1/NK.PF
	Begründung: „*Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN).*“ → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „*The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects … and the subjects application connector and workstation (German: Clientsystem) communicating with the TOE from its LAN interface (PS2) …*“ FDP_IFF.1/NK.PF modelliert einen Paketfilter („*…the decision shall be based on the following security attributes: IP address, port*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	number, and protocol type.“, „*For every operation (...) the TOE shall maintain a set of packet filtering rules ...*“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (*Stateful Packet Inspection*) abgebildet und durch das folgende Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen. FMT_SMR.1./NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf. *„Für zu schützende Daten der TI und der Bestandsnetze sowie zu schützende Nutzerdaten bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Clientsystemen) auf das Transportnetz wird durch den EVG unterbunden: IT-Systeme im LAN können nur unter der Kontrolle des EVG und im Einklang mit der Sicherheitspolitik des EVG zugreifen.*“ → Dies wurde teilweise durch FDP_IFF.1.3/NK.PF modelliert (zwangsweise Nutzung des VPN-Tunnels). Ferner ist die Sicherheitsleistung des Paketfilters natürlich abhängig von den verwendeten Paketfilterregeln. Daher beschränkt der EVG die Administration gewisser grundlegender Paketfilterregeln; siehe dazu das Refinement zu FMT_MSA.1/NK.PF. Für die Paketfilterregeln, die der Administrator administrieren darf, informiert ihn die Benutzerdokumentation hinreichend; siehe dazu das Refinement zu AGD_OPE.1 (Administration der Paketfilter-Regeln) in Abschnitt 6.2.8.	

Tabelle 30: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 205: Hinweis zu O.NK.VPN_Integrität: Zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash wird eine Hashfunktion verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruht, es sind daher keine entsprechenden geheimzuhaltenden Schlüssel erforderlich.

6.5.6. Detaillierte Erklärung für die Sicherheitsziele des Anwendungskonnektors

O.AK.Basis_Krypto

Das Sicherheitsziel O.AK.Basis_Krypto “Kryptographische Algorithmen“ fordert die Verwendung von sicheren kryptographischen Algorithmen und Protokollen im gesamten EVG,

die den normativen Anforderungen gemäß [12] für Signaturen und [19] bzw. [30] für Kryptoalgorithmen entsprechen. Dies ist in den folgenden SFRs umgesetzt:

- FCS_CKM.1/AK.AES fordert die kryptographische Schlüsselgenerierung von 128 und 256 Bit Schlüsseln gemäß [19].
- FCS_CKM.1/NK.TLS fordert die kryptographische Schlüsselgenerierung von 128 und 256 Bit Schlüsseln gemäß [30].
- FCS_CKM.4/AK fordert die Zerstörung von kryptographischen Schlüsseln.
- FCS_COP.1/AK.AES fordert die Verwendung von AES -256 zur symmetrischen Verschlüsselung und die Verwendung von AES-128 , AES-192 und AES-256 zur symmetrischen Entschlüsselung.
- FCS_COP.1/AK.CMS.Ent fordert die symmetrische Entschlüsselung von Dokumenten mit AES-256.
- FCS_COP.1/AK.CMS.SigPr fordert die Verwendung der Algorithmen CAdES, SHA-2 und RSA zur Verwendung bei der Prüfung signierter CMS-Dokumente.
- FCS_COP.1/AK.CMS.Sign fordert die Verwendung der Algorithmen CAdES und SHA-2 zur Verwendung bei der Erzeugung elektronischer Signaturen von Dokumenten.
- FCS_COP.1/AK.CMS.Ver fordert die Verwendung der Algorithmen AES-256 sowie RSA zur hybriden Verschlüsselung von Dokumenten.
- FCS_COP.1/NK.TLS.HMAC fordert die Verwendung des HMAC Verfahrens mit SHA-1 zum Berechnen und Prüfen von HMACs.
- FCS_COP.1/AK.PDF.SigPr und FCS_COP.1/AK.PDF.Sign fordern die Verwendung der Algorithmen PAdES, SHA-2 und RSA zur Prüfung und Erzeugung von signierten PDF-A Dokumenten.
- FCS_COP.1/AK.SigVer.PSS und FCS_COP.1/AK.SigVer.SSA fordern die Verwendung des Algorithmus RSA zur Prüfung digitaler Signaturen.
- FCS_COP.1/AK.SHA fordert die Verwendung des Algorithmus SHA-2 zur Berechnung von Hash-Werten.
- FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.Auth fordern die Verwendung der Algorithmen ECC, RSA, AES und SHA für die Absicherung der TLS-Kanäle.
- FCS_COP.1/AK.XML.Ent fordert die Verwendung der Algorithmen AES-256 zur symmetrischen Entschlüsselung von XML-Dokumenten.
- FCS_COP.1/AK.XML.Sign fordert die Verwendung der Algorithmen XAdES sowie SHA-2 im Zusammenwirken mit Signatur-Chipkarten zur Erzeugung von XML-Signaturen.
- FCS_COP.1/AK.XML.SigPr fordert die Verwendung der Algorithmen XAdES sowie SHA-2 und RSA zur Prüfung von XML-Signaturen.
- FCS_COP.1/AK.XML.Ver fordert die Verwendung der Algorithmen AES-256 sowie RSA für die hybride Verschlüsselung von XML-Dokumenten.

O.AK.Admin

Das Sicherheitsziel O.AK.Admin „Administration“ fordert die Einschränkung administrativer Funktionen auf besonders berechtigte Administratoren, insbesondere für das Management der eHealth-Kartenterminals und der Arbeitsplätze. Dies ist durch folgende SFR umgesetzt:

- FMT_SMR.1/**AK** listet die bekannten Rollen, darunter die Administrator-Rolle.
- FMT_SMF.1/**AK** listet die administrativen Funktionen, die alle in O.Admin gelisteten Bereiche erfassen.
- FMT_MOF.1/**AK** begrenzt die Aktivierung und Deaktivierung der Online Kommunikation, des Signaturdienstes und der Logischen Separation auf den Administrator.
- FIA_UAU.1/**AK** verbietet die Ausführung administrativer Funktionen vor erfolgreicher Authentisierung.
- FIA_UAU.5/**AK** fordert einen Passwort-Authentisierungsmechanismus für Administratoren.
- FDP_ACC.1/AK**.SDS** beschreibt die Zugriffskontrolle auf den sicheren Datenspeicher. Dabei bildet der Administrator ein Subjekt, das auf Daten oder Schlüssel dieses Datenspeichers zugreift.
- FDP_ACF.1/AK**.SDS** definiert die Zugriffskontrolle für den sicheren Datenspeicher.
- FIA_SOS.1/AK**.Passwörter** setzt eine Qualitätsmetrik für die Passwörter der Administratoren durch.
- FMT_MSA.1/AK**.TLS** beschreibt die Einschränkungen beim Verwalten von Sicherheitsattribute für TLS Kanälen. FMT_MSA.3/AK**.TLS** beschreibt den Umgang mit Standardwerten für Sicherheitsattribute von TLS-Kanälen.
- FMT_MTD.1/AK**.Zert** beschreibt und begrenzt die administrativen Funktionen für das CVC-Management auf den berechtigte Benutzer.
- FMT_MTD.1/AK.eHKT_**Abf** beschreibt und begrenzt die administrativen Funktionen für die Abfrage der Konfigurationsdaten der eHealth-Kartenterminals auf den S_AK und Administrator.
- FMT_MTD.1/AK.eHKT_**Mod** beschreibt und begrenzt die administrativen Funktionen für die Modifikation der Konfigurationsdaten der eHealth-Kartenterminals auf den Administrator.
- FMT_MTD.1/AK**.Admin** beschreibt und begrenzt die administrativen Funktionen für die Modifikation von Rollen, Konfigurationsdaten, zu protokollierende Ereignisse und Standardvorgaben für Signaturvorgänge sowie für das Modifizieren von EVG-Software und den Export und Import von Konfigurationsdaten auf den Administrator.
- FAU_GEN.1/AK erzeugt Protokolldaten über die Verschlüsselung von Dateien nach Verschlüsselungsrichtlinie,
- FAU_SAR.1/AK ermöglicht autorisierten Benutzern die Protokollaufzeichnungen in geeigneter Weise zu lesen.
- FAU_STG.1/AK schützt die Protokollaufzeichnungen gegen nichtautorisiertes Löschen und Modifizieren.
- FAU_STG.4/AK überschreibt die ältesten Protokolleinträge, wenn der Protokollspeicher voll ist.

O.AK.EVG_Modifikation

Das Sicherheitsziel O.AK.EVG_Modifikation „Schutz vor Veränderungen“ fordert vom EVG dem Nutzer zur Laufzeit sicherheitstechnische Veränderungen anzuzeigen und dauerhaft gespeicherte geheime kryptographische Schlüssel vor Kompromittierung durch physische und logische Angriffe zu schützen. Dies ist durch folgende SFR umgesetzt:

- FIA_UID.1/**AK** erlaubt den Selbsttest gemäß FPT_TST.1/Out-Of-Band vor der Identifizierung eines Benutzers.
- FPT_TST.1/AK**.Out-Of-Band** fordert, dass die TSF auf Anforderung eines autorisierten Benutzers eine Testfolge als Nachweis für den korrekten Betrieb der TSF durchführen muss.
- FPT_TST.1/AK**.Run-Time** fordert, dass die TSF auf regelmäßig während des Normalbetriebs eine Testfolge als Nachweis für den korrekten Betrieb der TSF durchführen muss.
- FPT_FLS.1/**AK** fordert den Übergang in einen sicheren Zustand, wenn Fehler erkannt wurden.
- FDP_RIP.1/**AK** fordert, dass die TSF sicherstellen muss, dass der frühere Informationsinhalt einer Ressource mit geheimen kryptographischen Schlüsseln bei Wiederfreigabe einer Ressource nicht verfügbar ist.

O.AK.IFD-Komm

Das Sicherheitsziel O.AK.IFD-Komm “Schutz der Kommunikation mit den eHealth-Kartenterminals“ fordert von dem EVG, die eHealth-Kartenterminals, mit denen er gepaart ist, zu authentisieren und die Vertraulichkeit und Integrität seiner Kommunikation mit den eHealth-Kartenterminals durch einen entsprechend gesicherten Kanal zu schützen. Der EVG verwendet selbst nur sichere kryptographische Algorithmen gemäß [19] für die TLS-Kanäle. Dieser Teil des Sicherheitsziels ist durch folgende SFR umgesetzt:

- FTP_ITC.1/AK**.eHKT** fordert die Einrichtung eines vertrauenswürdigen Kanals zwischen dem EVG und der sichere Signaturerstellungseinheit, der gemäß FDP_UCT.1/AK**.TLS** die Vertraulichkeit und gemäß FDP_UIT.1/AK**.TLS** die Integrität des Datenaustausches zu gewährleisten hat.
- FCS_CKM.1/NK.TLS fordert die Generierung kryptographischer Schlüssel nach Normen für TLS-Kanäle, insbesondere die Schlüsselgenerierung von AES-Schlüsseln, für die die Einsatzumgebung die benötigten Zufallszahlen erzeugt.
- Das Schlüsselmanagement muss die sichere Zerstörung der kryptographischen Schlüssel gemäß FCS_CKM.4/AK implementieren.
- Die kryptographischen Operationen des TLS-Kanals müssen gemäß FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.Auth mit den dort geforderten Algorithmen erfolgen.
- FPT_TEE.1/**AK** fordert bei der Herstellung einer Kommunikation mit einem Gerät, das vorgibt, ein eHealth-Kartenterminal zu sein, zu prüfen, ob das Gerät tatsächlich über

eine gesteckte gültige gSMC-KT verfügt, und das eHealth-Kartenterminal dem EVG als zulässiges Kartenterminal im LAN des Leistungserbringers bekannt ist.

- Diese Prüfung bei Verbindungsaufnahme zwischen dem EVG und den eHealth-Kartenterminals schließt eine Authentisierung nach TLS-Protokoll mit Pairing-Geheimnis gemäß FIA_UAU.5/**AK**. Die dafür präsentierten CV-Zertifikate werden gemäß FPT_TDC.1/**AK** auf Gültigkeit für gSMC-KT geprüft. Das Pairing-Geheimnis wird gemäß FIA_SOS.2/AK**.PairG** erzeugt.
- Die Ressourcen, die geheime kryptographische Schlüssel oder Benutzerdaten enthielten, die über den TLS-Kanal zwischen EVG und eHealth-Kartenterminals übermittelt wurden, müssen gemäß FDP_RIP.1/**AK** bei der Wiederfreigabe aufbereitet werden.
- FMT_MTD.1/AK.eHKT_**Abf**, FMT_MTD.1/AK.eHKT_**Mod** und FMT_MTD.1/AK**.Admin** fordern die Einrichtung administrativer Funktionen zur Verwaltung der eHealth-Kartenterminals auf den Administrator zu beschränken.
- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen für die eHealth-Kartenterminals sind durch FMT_SMF.1/**AK** gefordert.

O.AK.IFD-Komm

Das Sicherheitsziel O.AK.IFD-Komm sieht weiterhin vor, dass der EVG einen hinsichtlich Vertraulichkeit und Integrität geschützten Kanal zum Kartenterminal bereitstellt und dessen Nutzung kontrolliert. Dieser Teil des Sicherheitsziels ist durch folgende SFR umgesetzt:

- FDP_ACC.1/AK**.eHKT** führt die Kartenterminal SFP ein, die die Nutzung des TLS-Kanals zwischen dem EVG und den eHealth-Kartenterminals durch SICCT-Kommandos adressiert.
- FDP_ACF.1/AK**.eHKT** fordert eine Zugriffskontrolle für die Verwendung von SICCT-Kommandos, die die Nutzung kryptographischer Schlüssel auf Dienste des EVG und Anzeigen zur QES.

O.AK.Chipkartendienst

Das Sicherheitsziel O.AK.Chipkartendienst “Chipkartendienste des EVG“ fordert, Chipkarten an der ICCSN und den in den Chipkarten enthaltenen Angaben zu identifizieren, Chipkarten (außer KVK) mit Hilfe der Zertifikate auf der Chipkarte zu authentisieren, und einen Sicherheitsdienst zur gegenseitigen Authentisierung zwischen Chipkarten (Card-to-Card-Authentisierung) in den angeschlossenen eHealth-Kartenterminals bereit zu stellen.

- FPT_TEE.1/**AK** fordert bei Stecken einer Chipkarte, die vorgibt, ein HBA, eine gSMC-KT, eine SMC-B oder eine eGK zu sein, zu prüfen, ob sie tatsächlich eine solche Chipkarte ist. Die dafür präsentierten CV-Zertifikate werden gemäß FPT_TDC.1/**AK** auf Gültigkeit für HBA, SMC (gSMC-KT oder SMC-B) und eGK geprüft.
- FIA_UAU.5/**AK** fordert die Unterstützung der Authentisierung von Chipkarten auf der Basis von CV-Zertifikate, deren Gültigkeit gemäß FPT_TDC.1/**AK** zu prüfen sind, und die Authentisierung von SMC und HBA in der jeweils benötigten Rolle.

- Der EVG muss Funktionen zur Administration der Arbeitsplatzkonfiguration gemäß FMT_MTD.1/AK**.Admin** und der für die Chipkartenauthentisierung benutzten CV-Zertifikate gemäß FMT_MTD.1/AK**.Zert** bereitstellen.
- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen für die Cross-CVC sind durch FMT_SMF.1/**AK** gefordert.

Der EVG gewährt den Zugriff auf Chipkarten in Abhängigkeit von deren Sicherheitszustand und der Sicherheitspolitik des Anwendungsfalls.

- Der EVG kontrolliert den Zugriff auf Chipkartenkommandos der Chipkarten (außer PIN-Kommandos und kryptographische Schlüssel) über den Chipkartendienst gemäß FDP_ACC.1/AK**.KD** und FDP_ACF.1/AK**.KD**.
- Der EVG kontrolliert den Zugriff auf PIN-Kommandos der Chipkarten über den Chipkartendienst gemäß FDP_ACC.1/AK**.PIN** und FDP_ACF.1/AK**.PIN**.

O.AK.VAD

Das Sicherheitsziel O.AK.VAD "Schutz der Authentisierungsverifikationsdaten" definiert die Aufgaben des EVG bei der Steuerung und Zugriffskontrolle für die lokale und entfernte Eingabe von Authentisierungsverifikationsdaten der Benutzer der Chipkarten.

Insbesondere fordert es, dass der EVG den Benutzer der entfernten Eingabe bei der Identifizierung des zu benutzenden PIN-Terminals durch die sichere Bereitstellung einer hinreichend eindeutigen Jobnummer für das Clientsystem und der späteren Anzeige der vom Clientsystem übergebenen Jobnummer am PIN-Terminal, die dem identifizierten Arbeitsplatz zugeordnet ist.

- Die Erzeugung der Jobnummer ist durch FIA_SOS.2/AK**.Jobnummer** und deren Anzeige durch FTA_TAB.1/AK**.Jobnummer** gefordert.

Der EVG initiiert die Eingabe der Signatur-PIN und Signatur-PUK der Signaturschlüssel-Inhabers bzw. der Kartenhalter-PIN und Kartenhalter-PUK des Kartenhalters im sicheren PIN-Modus am PIN-Terminal und deren vertrauliche und integritätsgeschützte Übermittlung im Secure Messaging Kanal zwischen der SMC im PIN-Terminal zur VAD-empfangenden Chipkarte im Chipkarten-Terminal.

- Die Zugriffskontrolle für die lokale und entfernte PIN- und PUK-Eingabe ist durch FDP_ACC.1/AK**.PIN** und FDP_ACF.1/AK**.PIN** gefordert.
- FPT_TEE.1/**AK** fordert bei der Herstellung einer Kommunikation mit einem Gerät, das vorgibt, ein eHealth-Kartenterminal zu sein, zu prüfen, ob das Gerät tatsächlich über eine gültige gSMC-KT verfügt, und das eHealth-Kartenterminal dem EVG als zulässiges Kartenterminal im LAN des Leistungserbringers bekannt ist. FPT_TEE.1/**AK** fordert weiterhin, dass bei Stecken einer Chipkarte in ein eHealth-Kartenterminals, der Chipkartentyp als HBA, eine SMC, oder eGK und die CHA des CV-Zertifikats zu prüfen ist. Dadurch werden die Voraussetzungen für eine sichere lokale und entfernte PIN- und PUK-Eingabe sichergestellt.

- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen für die Cross-CV-Zertifikat sind durch FMT_SMF.1/**AK** gefordert.
- FIA_UAU.5/**AK** fordert Authentisierungsmechanismen für Chipkarten als PIN-Sender und PIN-Empfängen.
- FMT_MTD.1/AK**.Admin** fordert das Management der Arbeitsplatzkonfiguration, die das zugeordnete Clientsystem und eHealth-Kartenterminals einschließt, auf die Rolle des Administrators zu begrenzen.

O.AK.Enc

Das Sicherheitsziel O.AK.Enc "Verschlüsselung von Daten" fordert von dem EVG die automatische Verschlüsselung von Daten.

Diese Regeln werden durch den EVG gemäß folgender SFR umgesetzt:

- Verschlüsselung von Daten erfordert nach FIA_UAU.1/**AK** keine Benutzerauthentisierung.
- Die Zugriffskontrolle in Abhängigkeit von den Sicherheitsattributen der zu verschlüsselnden Daten wurde gemäß FDP_ACC.1/AK**.Enc** und FDP_ACF.1/AK**.Enc** durchgesetzt.
- Vor dem Verschlüsseln werden gemäß FDP_ITC.2/AK**.Enc** die Gültigkeit der Verschlüsselungsrichtlinie und der Zertifikate der Empfänger geprüft. Die CA-Zertifikate können durch den Administrator importiert werden.
- Für die Verschlüsselung selbst fordern die SFRs FCS_COP.1/AK.AES und FCS_COP.1/AK.CMS.Ver die Verwendung der Algorithmen AES bzw. AES mit RSA für Hybrid-Verschlüsselung. Ferner fordert FCS_COP.1/AK.XML.Ver die hybride Verschlüsselung von XML Dokumenten.
- Verschlüsselte Daten werden gemäß FDP_ETC.2/AK**.Enc** nur mit der Identität der vorgesehenen Empfänger und der Identität der verwendeten Verschlüsselungsrichtlinie ausgegeben.
- FDP_RIP.1/**AK** schützt zu verschlüsselnde Daten bei Wiederfreigabe einer Ressource.
- Die Gültigkeit der X.509-Verschlüsselungszertifikate wird gemäß FPT_TDC.1/**AK** geprüft.

Der EVG verwendet selbst nur sichere kryptographische Algorithmen gemäß [19] für die Verschlüsselung von Dokumenten, wobei

- FCS_CKM.1/AK.AES die Erzeugung der AES-Schlüssel fordert.
- FCS_CKM.4/AK die Bereitstellung von Verfahren zur sicheren Löschung der verwendeten Schlüssel und FDP_RIP.1/**AK** die Löschung zu verschlüsseln Dateien bei der Wiederfreigabe der Ressourcen fordern.

O.AK.Dec

Das Sicherheitsziel O.AK.Dec "Entschlüsselung von Daten" erlaubt dem EVG, Daten automatisch zu entschlüsseln, wenn dies die gültigen Verschlüsselungspolicy und der Sicherheitszustand der Chipkarten erlauben. Diese Regeln werden durch den EVG gemäß folgender SFR umgesetzt:

- Entschlüsselung von Daten erfordert nach FIA_UAU.1/**AK** keine Benutzerauthentisierung.
- Die Zugriffskontrolle in Abhängigkeit von den Sicherheitsattributen der zu entschlüsselnden Daten wurde gemäß FDP_ACC.1/AK**.Enc** und FDP_ACF.1/AK**.Enc** durchgesetzt.
- Zu entschlüsselnde Daten werden gemäß FDP_ITC.2/AK**.Enc** nur nach Prüfung der Gültigkeit der Verschlüsselungspolicy importiert.
- Für die Entschlüsselung selbst fordern die SFRs FCS_COP.1/AK.AES und FCS_COP.1/AK.CMS.Ent die Verwendung der Algorithmen AES bzw. AES mit RSA für Hybrid-Verschlüsselung. Ferner fordert FCS_COP.1/AK.XML.Ent die hybride Entschlüsselung von XML Dokumenten.
- Entschlüsselte Daten werden gemäß FDP_ETC.2/AK**.Enc** nur mit der Identität der vorgesehenen Empfänger, dessen Chipkarte zum Entschlüsseln benutzt wurde, ausgegeben.
- FDP_RIP.1/**AK** schützt entschlüsselte Daten bei Wiederfreigabe einer Ressource. Der EVG unterstützt selbst nur sichere kryptographische Algorithmen gemäß [19] für die Entschlüsselung von Dokumenten, wobei
- FCS_COP.1/AK.XML.Ent die Entschlüsselung von XML-Dokumenten fordert, und
- FCS_CKM.4/AK die Bereitstellung von Verfahren zur sicheren Löschung der verwendeten Schlüssel und FDP_RIP.1/**AK** die Löschung entschlüsselten Dateien bei der Wiederfreigabe der Ressourcen fordern.

O.AK.Protokoll

Das Sicherheitsziel O.AK.Protokoll "Sicherheitsprotokoll mit Zeitstempel" fordert die Protokollierung sicherheitsrelevanter Ereignisse durch den EVG. Der EVG protokolliert gemäß den folgenden SFR:

- FAU_GEN.1/AK erzeugt Protokolldaten über sicherheitsrelevante Ereignisse (bei solchen Ereignissen verbleibt der EVG aufgrund der SFR FPT_FLS.1/**AK** stets in einem sichern Zustand),
- FAU_SAR.1/AK ermöglicht autorisierten Benutzern die Protokollaufzeichnungen in geeigneter Weise zu lesen.
- FAU_STG.1/AK schützt die Protokollaufzeichnungen gegen nichtautorisiertes Löschen und Modifizieren.
- FAU_STG.4/AK überschreibt ältere Protokolleinträge, wenn das Protokoll voll ist.

O.AK.Sig.SignQES

Das Sicherheitsziel O.AK.Sig.SignQES "Signaturrichtlinie für qualifizierte elektronische Signaturen" fordert von dem EVG in Abhängigkeit von der gültigen Signaturrichtlinie die Erzeugung qualifizierter elektronischer Signaturen für bestimmte Datenformate nach Überprüfung der Wohlgeformtheit dieser zu signierenden Daten. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_ACC.1/AK**.Sgen** führt die Signaturerstellungs-SFP ein und FDP_ACF.1/AK**.Sgen** setzt sie in Abhängigkeit von der Signaturrichtlinie um.
- FDP_DAU.2/AK**.QES** fordert von der TSF, die Fähigkeit zur Erstellung signierter Daten mit qualifizierten elektronischen Signaturen mit Hilfe der sicheren Signaturerstellungseinheit bereitzustellen.
- FDP_DAU.2/AK**.Cert** fordert von der TSF, die Fähigkeit zur Erstellung von Nachweisen zur Gültigkeit von qualifizierten elektronischen Signaturen mit Hilfe von Zertifikaten bereitzustellen.
- FDP_ITC.2/AK**.Sig** fordert der TSF, zu signierende Daten und zu prüfende signierte Daten nur nach erfolgreicher Prüfung der Zulässigkeit der Signaturrichtlinie zu importieren.
- FPT_TDC.1/**AK** fordert die Unterstützung der Verteilung neuer öffentlicher Schlüssel über Trust--service Status Listen.
- FMT_MSA.3/AK**.Sig** schränkt das Management der Signaturrichtlinie auf den Administrator ein.
- Die TSF muss die Qualität des Administratorpasswortes gemäß FIA_SOS.1/AK**.Passwörter** und die Authentisierung des Administrators gemäß FIA_UAU.5/**AK** durchsetzen.
- FCS_COP.1/AK.SHA, FCS_COP.1/AK.XML.Sign, FCS_COP.1/AK.CMS.Sign und FCS_COP.1/AK.PDF.Sign fordern von der TSF, sichere kryptographische Algorithmen gemäß [19] für die Signaturerstellung zu implementieren.

O.AK.Sig.SignNonQES

Das Sicherheitsziel O.AK.Sig.SignNonQES "Signaturrichtlinie für nichtqualifizierte elektronische Signaturen" fordert von dem EVG die Erzeugung nichtqualifizierter elektronische Signaturen für bestimmte Datenformate nach Überprüfung der Wohlgeformtheit dieser zu signierender Daten. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_ACC.1/AK**.Sgen** führt die Signaturerstellungs-SFP ein und FDP_ACF.1/AK**.Sgen** setzt sie in Abhängigkeit von der Signaturrichtlinie um.
- FDP_DAU.2/AK**.Sig** fordert von der TSF, die Fähigkeit zur Erstellung signierter Daten mit nichtqualifizierten elektronischen Signaturen mit Hilfe der Chipkarten bereitzustellen.
- FCS_COP.1/AK.SHA, FCS_COP.1/AK.CMS.Sign und FCS_COP.1/AK.PDF.Sign fordern von der TSF sichere kryptographische Algorithmen gemäß [19] für die Signaturerstellung zu implementieren.

O.AK.Sig.exklusivZugriff

Das Sicherheitsziel O.AK.Sig.exklusivZugriff "Unterstützung bei alleiniger Kontrolle" fordert von dem EVG Methoden zur Verfügung zu stellen, die es dem Signaturschlüssel-Inhaber ermöglichen, die alleinige Kontrolle über die QSEE auszuüben. Diese Forderung ist durch FDP_ACC.1/AK**.Sgen** und FDP_ACF.1/AK**.Sgen** umgesetzt Zusätzlich unterstützen die folgenden SFRs die Umsetzung des Sicherheitszieles:

- Gemäß FDP_ACF.1/AK**.Sgen** und FMT_MSA.4/**AK** werden die Authentisierung des Signaturschlüsselinhabers gegenüber der sicheren Signaturerstellungseinheit und die Autorisierung des Signaturvorgangs für die angezeigten zu signierenden Daten erzwungen und die TSF darf nur für solche Dateien und Heilberufsausweise den Signaturprozess auslösen, die von dem autorisierten Benutzer des Clientsystems ausgewählt wurden. Außerdem überprüft die TSF, ob für diese Daten ordnungsgemäße qualifizierte elektronische Signaturen erstellt wurden.
- FMT_MSA.1/AK**.User** begrenzt das Recht zur Modifikation des Autorisierungsstatus zu signierender Dateien auf den Benutzer des Clientsystems.
- Die Zuordnung von Benutzer des Clientsystems und Signaturschlüssel-Inhaber wird durch FIA_SOS.2/AK**.Jobnummer** und FTA_TAB.1/AK**.Jobnummer** unterstützt.
- Die TSF muss die Integrität der zum Signieren vom EVG übergebenen Daten gemäß FDP_SDI.2/**AK** überwachen.
- FDP_RIP.1/**AK** fordert, zu signierende Daten und signierte Daten nach der Ausgabe bei Wiederfreigabe der Ressourcen zu löschen.
- FTP_ITC.1/AK**.**QSEE fordert die Einrichtung eines vertrauenwürdigen Kanals zwischen EVG und QSEE zum Schutz der zu signierenden Daten.
- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen für die Signaturrichtlinein sind durch FMT_SMF.1/**AK** gefordert.
- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen des EVG, insbesondere das Management der eHealth-Kartenterminals und der Arbeitsplätze, sind durch FMT_SMF.1/**AK** gefordert.

O.AK.Sig.Einfachsignatur

Das Sicherheitsziel O.AK.Sig.Einfachsignatur „Einfachsignatur" fordert von dem EVG die Unterstützung der Einfachsignatur. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_ACC.1/AK**.Sgen** identifiziert die Signaturerstellungs-SFP,
- FDP_ACF.1/AK**.Sgen** beschreibt Regeln für die Einfachsignatur,
- FIA_UAU.5/**AK** beschreibt die Forderung der Authentisierung des HBA vor Ausführung einer Einfachsignatur.

O.AK.Sig.Stapelsignatur

Das Sicherheitsziel O.AK.Sig.Stapelsignatur "Stapelsignatur" fordert von dem EVG die Unterstützung der Stapelsignatur gemäß [21]. Die Forderungen aus [21] werden insbesondere durch folgende SFR umgesetzt.

- FIA_API.1/**AK** fordert, dass die TSF sich gegenüber der QSEE für die Stapelsignatur authentisiert.
- FIA_UAU.5/**AK** beschreibt die Forderung der Authentisierung des HBA vor Ausführung einer Stapelsignatur, und außerdem den Schutz von Vertraulichkeit und Integrität der Kommunikation (insbesondere mit der QSEE) zu schützen.
- FDP_ACF.1/AK**.Sgen** und FMT_MSA.4/**AK** fordern von der TSF zu überprüfen, ob für die Daten des Stapels ordnungsgemäße qualifizierte elektronische Signaturen erstellt wurden. Bei festgestellten Abweichungen sind alle durch die aktuelle Signtaur-PIN-Eingabe autorisierte Signaturen zu verwerfen. FDP_ACC.1/AK**.Sgen** identifiziert die Signaturerstellungs-SFP.
- FDP_ACF.1/AK**.Sgen** fordert von der TSF, den Sicherheitszustand der QSEE, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers erlangt wurde, nach der Abarbeitung des Stapels zurückzusetzen.
- Das Clientsystem ist über festgestellte Abweichungen beim Signaturprozess über die Schnittstelle gemäß FTA_TAB.1/AK**.SP** zu informieren.
- FTP_ITC.1/AK**.**QSEE fordert die Einrichtung eines vertrauenwürdigen Kanals zwischen EVG und QSEE zum Schutz der zu signierenden Daten.

O.AK.Sig.Komfortsignatur

Das Sicherheitsziel O.AK.Sig.Komfortsignatur "Komfortsignatur" fordert von dem EVG die Unterstützung der Komfortsignatur. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FIA_API.1/**AK** fordert, dass die TSF sich gegenüber der QSEE für die Komfortsignatur authentisiert.
- FIA_UAU.5/**AK** beschreibt die Forderung der Authentisierung des HBA vor Aktivierung der Komfortsignatur und außerdem den Schutz von Vertraulichkeit und Integrität der Kommunikation (insbesondere mit der QSEE) zu schützen. Zudem fordert FIA_UAU.5/**AK** die Authentisierung des Clientsystems vor Durchführung einer Komfortsignatur.
- FDP_ACF.1/AK**.Sgen** und FMT_MSA.4/**AK** fordern von der TSF, den Sicherheitszustand der QSEE, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers bei Aktivierung der Komfortsignatur erlangt wurde, für eine HBA-Kartensitzung erst nach Ablauf eines Zählers oder Zeitwertes zurückzusetzen oder für alle HBAs bzw. HBA-Kartensitzungen bei expliziter Deaktivierung der Komfortsignatur.
- Das Clientsystem ist über festgestellte Abweichungen beim Signaturprozess über die Schnittstelle gemäß FTA_TAB.1/AK**.SP** zu informieren.

- FTP_ITC.1/AK**.**QSEE fordert die Einrichtung eines vertrauenwürdigen Kanals zwischen EVG und QSEE zum Schutz der zu signierenden Daten.

O.AK.Sig.PrüfungZertifikat

Das Sicherheitsziel O.AK.Sig.PrüfungZertifikat "Prüfung des Signatur-Zertifikates" fordert vom EVG, dass er die Gültigkeit dieser Zertifikate, auf denen die Signatur beruht, prüft. Diese Prüfung umfasst den Abgleich, ob die zum Signaturprüfungszeitpunkt verwendeten Signaturalgorithmen für qualifizierte Zertifikate gemäß [19] als kryptografisch sicher gelten bzw. galten. Das Ergebnis der Prüfung wird an der Schnittstelle zum Clientsystem zur Verfügung gestellt. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_DAU.2/AK**.QES** fordert die Prüfung der qualifizierten Zertifikate nach dem Kettenmodell.
- FDP_DAU.2/AK**.Cert** fordert die einzelnen für Zertifikate zu prüfenden Aspekte bei der Prüfung digitaler Signaturen.
- FDP_DAU.2/AK**.Sig** fordert die Prüfung nichtqualifizierter elektronischer Signaturen für die Benutzer gemäß gültiger Signaturrichtlinien bereitzustellen.
- FPT_TDC.1/**AK** fordert eine konsistente Interpretation der Zertifikate für die Prüfung qualifizierter elektronischer Signaturen bis zu einer bekannten Wurzel und nicht-qualifizierter X.509-Signaturzertifikate.
- Für die Prüfung der digitalen Signaturen der Zertifikate muss die TSF die kryptographischen Operationen gemäß FCS_COP.1/AK.SHA, FCS_COP.1/AK.SigVer.PSS und FCS_COP.1/AK.SigVer.SSA implementieren.
- FIA_UAU.1/**AK** und FDP_ACF.1/AK**.SigPr** erlauben gemäß FDP_ACC.1/AK**.**SigPr eingeführter Signaturprüfung-SFP die Signaturprüfung durch nichtauthentisierte Benutzer.
- FMT_MSA.3/AK**.Sig** schränkt das Management der Signaturrichtlinie, die insbesondere die Prüfung der Zertifikate bestimmt, auf den Administrator ein.

O.AK.Sig.Schlüsselinhaber

Das Sicherheitsziel O.AK.Sig.Schlüsselinhaber "Zuordnung des Signaturschlüssel-Inhabers" fordert vom EVG, bei der Überprüfung der signierten Daten anzuzeigen, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_DAU.2/AK**.QES**, FDP_DAU.2/AK**.Sig** und FDP_DAU.2/AK**.Cert** fordern die Fähigkeit der TSF zur Bereitstellung des Signaturschlüssel-Inhabers über die Schnittstelle des Clientsystems für qualifizierte und nichtqualifizierte elektronische Signaturen sowie für Signaturen in elektronischen Zertifikaten.
- FPT_TDC.1/**AK** fordert eine konsistente Interpretation der Zertifikate (die den Signaturschlüssel-Inhaber identifizieren) für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierter X.509-Signaturzertifikate sowie deren Prüfung bis zu einer bekannten Wurzel.

- FIA_UAU.1/**AK** und FDP_ACF.1/AK**.SigPr** erlauben gemäß FDP_ACC.1/AK**.**SigPr eingeführter Signaturprüfung-SFP die Signaturprüfung durch nichtauthentisierte Benutzer.

O.AK.Sig.SignaturVerifizierung

Das Sicherheitsziel O.AK.Sig.SignaturVerifizierung "Verifizierung der Signatur" fordert vom EVG die Korrektheit einer digitalen Signatur zuverlässig zu prüfen und das Ergebnis der Prüfung an der Schnittstelle zum Clientsystem zur Verfügung zu stellen. Bei der Überprüfung der signierten Daten zeigt der EVG an, ob die signierten Daten unverändert sind. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_DAU.2/AK**.QES** fordert die Prüfung der qualifizierten elektronischen Signaturen, hier speziell der signierten Daten, nach dem Kettenmodell.
- FDP_DAU.2/AK**.Cert** fordert die einzelnen für die signierten Daten zu prüfenden Aspekte bei der Prüfung digitaler Signaturen.
- FDP_DAU.2/AK**.Sig** fordert die Prüfung nichtqualifizierter elektronischer Signaturen für die Benutzer gemäß gültiger Signaturrichtlinien bereitzustellen.
- Für die Prüfung der digitalen Signaturen der signierten Daten muss die TSF die kryptographischen Operationen gemäß FCS_COP.1/AK.SHA, FCS_COP.1/AK.SigVer.PSS, , FCS_COP.1/AK.SigVer.ECDSA und FCS_COP.1/AK.SigVer.SSA implementieren.
- Für die Prüfung der XML-kodierten signierten Daten muss die TSF FCS_COP.1/AK.XML.SigPr implementieren. Für CMS bzw. PKCS#1 kodierte signierte Dokumente ist dies entsprechend in FCS_COP.1/AK.CMS.SigPr gefordert. Für die Prüfung signierter PDF-Dokumente muss die TSF FCS_COP.1/AK.PDF.SigPr implementieren.
- FIA_UAU.1/**AK** und FDP_ACF.1/AK**.SigPr** erlauben gemäß FDP_ACC.1/AK**.**SigPr eingeführter Signaturprüfung-SFP die Signaturprüfung durch nichtauthentisierte Benutzer.

O.AK.Selbsttest

Das Sicherheitsziel O.AK.Selbsttest „Selbsttests" fordert vom EVG die Durchführung von Selbsttests beim Start-up und bei Bedarf. FPT_TST.1/AK**.Run-Time** fordert die Durchführung einer Testfolge beim Erstanlauf und regelmäßig während des Normalbetriebes des EVG. Ferner fordert FPT_TST.1/AK**.Out-Of-Band** die Durchführung einer Testfolge auf Anforderung durch den Benutzer. Dadurch kann die Integrität der TSF-Daten überprüft werden. Bei gefundenen Fehlerzuständen verbleibt der EVG aufgrund FPT_FLS.1/**AK** stets in einem sicheren Zustand.

O.AK.LAN

Das Sicherheitsziel O.AK.LAN „gesicherte Kommunikation im LAN der Leistungserbringer" fordert vom EVG die Möglichkeit einer bezüglich Integrität, Authentizität und Vertraulichkeit

gesicherten Verbindung zwischen EVG und Clientsystemen. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FTP_ITC.1/AK**.CS** fordert einen vertrauenswürdigen Kanal zwischen dem EVG und Clientsystemen.
- Die kryptographischen Operationen des TLS-Kanals müssen gemäß FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.Auth mit den dort geforderten Algorithmen erfolgen.
- FCS_CKM.1/NK.TLS fordert die kryptographische Schlüsselgenerierung von 128 und 256 Bit Schlüsseln gemäß [68] und [19].
- FDP_ACC.1/AK**.TLS** führt die TLS-SFP ein und FDP_ACF.1/AK**.TLS** definiert die Regeln des Zugriffs auf TLS Kanäle und die damit transportierten Daten.
- FMT_MSA.1/AK**.TLS** beschreibt die Einschränkungen beim Verwalten von Sicherheitsattribute für TLS Kanälen. FMT_MSA.3/AK**.TLS** beschreibt den Umgang mit Standardwerten für Sicherheitsattribute von TLS-Kanälen.
- FCS_CKM.1/NK.Zert fordert die Erzeugung von X.509 Zertifikaten von Clientsystemen zur Absicherung der TLS-Verbindungen. Diese können mittels FDP_ETC.2/NK.TLS zur Verwendung in Clientsystemen exportiert werden. FDP_ITC.2/NK.TLS ermöglicht dem Import von X.509 Zertifikaten von Clientsystemen.

O.AK.WAN

Das Sicherheitsziel O.AK.WAN „gesicherte Kommunikation zwischen EVG und Fachdiensten“ fordert vom EVG die Möglichkeit einer bezüglich Integrität, Authentizität und Vertraulichkeit gesicherten Verbindung zwischen EVG und Fachdiensten. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FTP_ITC.1/AK**.FD** fordert einen vertrauenswürdigen Kanal zwischen dem EVG und Fachdiensten.
- Die kryptographischen Operationen des TLS-Kanals müssen gemäß FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.Auth mit den dort geforderten Algorithmen erfolgen.
- FDP_ACC.1/AK**.TLS** führt die TLS-SFP ein und FDP_ACF.1/AK**.TLS** definiert die Regeln des Zugriffs auf TLS Kanäle und die damit transportierten Daten.
- FMT_MSA.1/AK**.TLS** beschreibt die Einschränkungen beim Verwalten von Sicherheitsattributen für TLS Kanälen. FMT_MSA.3/AK**.TLS** beschreibt den Umgang mit Standardwerten für Sicherheitsattribute von TLS-Kanälen.

O.AK.Zeit

Das Sicherheitsziel O.AK.Zeit „Systemzeit“ fordert vom EVG die Bereitstellung einer sicheren Systemzeit, die in regelmäßigen Abständen (vom Netzkonnektor) mit einem vertrauenswürdigen Zeitdienst synchronisiert wird. FPT_STM.1/**AK** fordert die Bereitstellung

eines verlässlichen Zeitstempels. Details zur Synchronisation der Systemzeit sind Aufgabe des Netzkonnektors und in dessen Schutzprofil [17] definiert.

O.AK.Update

Das Sicherheitsziel O.AK.Update „Software Update und Update von TSL, CRL und BNetzA-VL“ fordert vom EVG die Aktualisierung von Software-Komponenten und von TSL, BNetzA-VL und CRL, deren Prüfung auf Integrität, sowie die Übertragung der BNetzA-VL, deren Hash und von Firmware-Update-Paketen über einen sicheren Kanal. FDP_ACC.1/AK**.Update** führt die Update-SFP für den Software-Update ein und FDP_ACF.1/AK**.Update** definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_UIT.1/AK**.Update** fordert den Empfang der Software-Update-Daten und die Prüfung der Integrität dieser Daten vor dem Update. Die Anforderungen FTP_ITC.1/AK.KSR und FTP_TRP.1/NK.Admin fordern einen gesicherten Kanal für den Empfang der Software-Update-Daten aus der TI bzw. lokal über die Management-Schnittstelle. FPT_TDC.1/**AK** fordert die Fähigkeit des EVG zur Interpretation, und damit dem Import und die Aktualisierung von TSL und CRL nach erfolgreicher Prüfung der entsprechenden Signaturen und Zertifikate. FTP_ITC.1/AK.KSR und FTP_ITC.1/AK.TSL fordern den Aufbau eines sicheren Kanals für den Download von Firmware-Update-Paketen bzw. der BNetzA-VL und deren Hash-Wert.

O.AK.exklusivZugriff

Das Sicherheitsziel O.AK.exklusivZugriff „Alleinige Kontrolle von Terminal und Karte“ fordert vom EVG die Bereitstellung von Methoden, die es dem Benutzer ermöglichen, die alleinige Kontrolle über die verwendeten Kartenterminals und die verwendeten Chipkarten auszuüben. FDP_ACC.1/AK.**Infomod** führt die Infomodell-SFP ein und FDP_ACF.1/AK**.Infomod** definiert die Regeln des Zugriffs auf Kartenterminals und Kartensitzungen. Ferner werden in FDP_ACF.1/AK**.KD** Regeln zur Zugriffskontrolle auf Chipkarten und Kommunikationskanäle mit Chipkarten definiert.

O.AK.PinManagement

Das Sicherheitsziel O.AK.PinManagement „Management von Chipkarten-PINs“ fordert vom EVG die Möglichkeit zum Ändern, Aktivieren und Deaktivieren von PINs der Chipkarten, das Abfragen der Status von PINs der Chipkarten sowie das Entsperren gesperrter Chipkarten-PINs. FDP_ACC.1/AK**.PIN** führt die VAD-SFP ein und FDP_ACF.1/AK**.PIN** definiert die Regeln für den Umgang, die Eingabe und dem Wechsel mit Chipkarten-PINs.

O.AK.Infomodell

Das Sicherheitsziel O.AK.Infomodell „Umsetzung des Informationsmodells durch den EVG“ fordert vom EVG die persistente Zuordnung von Mandanten, Clientsystemen, Arbeitsplätzen und Kartenterminals sowie die transiente Zuordnung von Benutzern zu Arbeitsplätzen. Ferner fordert es die Verwaltung in Kartenterminals gesteckter Chipkarten und Kartensitzungen zur

Durchsetzung einer Zugriffskontrolle über die den Mandanten zugeordneten Ressourcen, die Chipkarten der Benutzer der Arbeitsplätze und die Chipkarten in Übereinstimmung der für die Kartensitzung erreichten Sicherheitszustände. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FDP_ACC.1/AK.**Infomod** führt die Infomodell-SFP ein und FDP_ACF.1/AK**.Infomod** definiert die Regeln für den Zugriff und die Verwaltung von Kartenterminals, Kartensitzungen, Karten, Arbeitsplätzen, Mandanten und Clientsystemen.
- FMT_MSA.1/AK**.Infomod** beschreibt die Einschränkungen beim Verwalten von persistenten Sicherheitsattributen im Informationsmodell des Konnektors. FMT_MSA.3/AK**.Infomod** beschreibt den Umgang mit Standardwerten für Sicherheitsattribute im Informationsmodell des Konnektors.

Sollte dennoch der EVG durch einen festgestellten Verstoß gegen das Infomodell in einen Fehlerzustand gelangen, so verbleibt der EVG aufgrund des SFR FPT_FLS.1/**AK** stets in einem sicheren Zustand.

O.AK.VSDM

Das Sicherheitsziel O.AK.VSDM „Versichertenstammdatenmanagement“ enthält Anforderungen an den EVG zum Verhalten des VSDM Fachmodules und zur Kommunikation mit dem VSDD Fachdienst. Diese werden durch die SFRs FDP_ACC.1/AK**.VSDM** und FDP_ACF.1/AK**.VSDM** umgesetzt: FDP_ACC.1/AK**.VSDM** führt die VSDM-SFP für den Zugriff auf Versichertenstammdaten ein und FDP_ACF.1/AK**.VSDM** definiert die Regeln für den Zugriff auf Versichertenstammdaten und für die Kommunikation mit dem VSDD Fachdienst; das Management der Sicherheitsattribute von FDP_ACF.1/AK**.VSDM** geschieht über FMT_MSA.1/AK**.VSDM** und FMT_MSA.3/AK**.VSDM**. Die TLS-Verbindung zwischen VSDM-Fachmodul und VSDD Fachdienst gemäß FTP_ITC.1/AK**.FD** unterliegt der Zugriffskontrolle gemäß FDP_ACC.1/AK**.TLS** und FDP_ACF.1/AK**.TLS** sowie dem Management gemäß FMT_MSA.1/AK**.TLS** und FMT_MSA.3/AK**.TLS**.

O.AK.VZD

Das Sicherheitsziel O.AK.VZD „Kommunikation mit dem zentralen Verzeichnisdienst“ werden gesicherte Kanäle zwischen dem LDAP-Proxy und dem VZD bereit gestellt. Diese TLS-Kanäle werden gemäß SFR FTP_ITC.1/AK**.VZD** implementiert und unterliegen der Zugriffskontrolle gemäß FDP_ACC.1/AK**.TLS** und FDP_ACF.1/AK**.TLS** sowie dem Management gemäß FMT_MSA.1/AK**.TLS** und FMT_MSA.3/AK**.TLS**.

O.AK.VAUSGD

Das Sicherheitsziel O.AK.VAUSGD (Anteil VAU) stellt VAU-Kanäle zur sicheren Kommunikation mit der Vertrauenswürdigen Ausführungsumgebung (VAU) der ePA

Fachanwendung zur Verfügung. Diese VAU-Kanäle werden gemäß SFR FTP_ITC.1/VAU implementiert. Das VAU-Protokoll ist dabei eine entsprechend FCS_CKM.1/VAU, FCS_COP.1/VAU.AES und FCS_CKM.4/AK modellierte Sicherungsschicht innerhalb eines TLS-Kanals. Die Authentisierung ist zertifikatsbasiert (FCS_COP.1/VAU.Auth) und folgt den Regeln in FPT_TDC.1/SGDVAU.

Das Sicherheitsziel O.AK.VAUSGD (Anteil SGD) stellt eine Ende zu Ende Verschlüsselung von SGD-Client und den SGD-HSMs der Schlüsselgenerierungsdienste SGD1 und SGD2 der ePA Fachanwendung dar. Dabei werden einzelne Nachrichtenteile des SGD-Protokolls so verschlüsselt, dass sie nur vom jeweiligen HSM entschlüsselt werden können. Dieser gesicherte Anteil der Kommunikation wird entsprechend dem SFR FTP_ITC.1/SGD als SGD-Kanal aufgefasst. Der SGD-Kanal ist dabei entsprechend FCS_COP.1/SGD.ECIES und FCS_CKM.4/AK modelliert und setzt auf ECIES-Verschlüsselung auf. Der öffentliche ECIES-Schlüssel des HSM wird dazu zusammen mit seiner Signatur und dem entsprechenden Zertifikat mittels *GetPublicKey* Operation eingebracht (FDP_ITC.2/SGD). Die Verwendung des Schlüssels ist nur erlaubt, wenn die Prüfung der Signatur und des Zertifikates erfolgreich sind (FDP_ACC.1/SGD, FDP_ACF.1/SGD). Die Authentisierung ist zertifikatsbasiert (FCS_COP.1/SGD.Auth) und folgt den Regeln in FPT_TDC.1/SGDVAU.

6.5.7. Erklärung für die Vertrauenswürdigkeitsanforderungen

Der Schutz der Benutzerdaten durch Verschlüsselung erfordert einen Schutz gegen ein Angriffspotential „Enhanced Basic“. Für CC Version 3.1 ist folglich eine Erweiterung der gewählten EAL-Stufe EAL3 um AVA_VAN.3 notwendig. Daraus ergeben sich Abhängigkeiten gem. [6], die mit den zusätzlichen Erweiterung um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 und ALC_TAT.1 aufgelöst werden.

Anmerkung: Die in CC Teil 3 [6] angegebenen Abhängigkeiten von AVA_VAN.3 sind leider nicht vollständig aufgelöst: ADV_IMP.1 impliziert zusätzlich ALC_TAT.1.

Die Komponente ALC_FLR.2 wurde gewählt, um Prozeduren zur Beseitigung von festgestellten Sicherheitsproblemen und Verbesserungen des EVG auf der Grundlage von Informationen der Anwender reagieren zu können und zur Verbesserung des EVG beizutragen. ALC_FLR.2 besitzt keine weiteren Abhängigkeiten.

Die EAL-Stufe an sich ist in sich konsistent und erfüllt alle Abhängigkeiten.

7. Zusammenfassung der EVG Sicherheitsfunktionalität

7.1. Sicherheitsfunktionen des Netzkonnektors

Die funktionalen Sicherheitsanforderungen werden im Folgenden nach funktionalen Gruppen gegliedert. Die funktionalen Gruppen orientieren sich an den in Abschnitt 1.3.5 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

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

7.1.1. NK.VPN-Client

VPN

Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt (Bei Verbindungen zum *VPN-Konzentrator der Telematikinfrastruktur* siehe FTP_ITC.1/NK.VPN_TI und bei Verbindungen zum *Sicheren Internet Service (SIS)* siehe FTP_ITC.1/NK.VPN_SIS). Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei wird IKEv2 unterstützt.

Informationsflusskontrolle

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

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

Diese Aspekte ergeben sich aus der Betrachtung der VPN-Kanäle. Sie werden aber im Hinblick auf ihre Realisierung der Anforderung nach Informationsflusskontrolle mittels einem dynamischen Paketfilter (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, siehe Abschnitt 6.2.2) zugeordnet.

Durch FDP_IFF.1.2/NK.PF wird eine VPN-Nutzung für *zu schützende Daten der TI und der Bestandsnetze* und für *zu schützende Nutzerdaten* (im Sinne des Abschnitts 3.1) gefordert, sofern die Paketfilter-Regeln geeignet gesetzt sind. Dies wird durch die Administratordokumentation (siehe das Refinement zu AGD_OPE.1 in Abschnitt 6.2.8) sichergestellt.

7.1.2. NK.Dynamischer Paketfilter

Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird als Informationsflusskontrolle modelliert (siehe FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF). Zur zustandsgesteuerten Filterung siehe auch Abschnitt 7.1.4 Stateful Packet Inspection.

Die von FDP_IFF.1.2/NK.PF geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (siehe FMT_MSA.3/NK.PF) und können vom Administrator verwaltet werden (siehe FMT_MSA.1/NK.PF, vgl. Abschnitt 6.2.6 Administration).

7.1.3. NK.Netzdienste

Zeitsynchronisation

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

Der EVG unterstützt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand an der Außenhaut des Konnektors anzeigt, um die Anforderung gemäß Konnektor-Spezifikation [27], Abschnitt 3.3 *Betriebszustand* umzusetzen, siehe LS14 und PS5 in Kapitel 1.3.3 sowie die Anforderungen an die Konnektor Hardware in Kapitel 1.3.6.

Zertifikatsprüfung

Der EVG überprüft die Gültigkeit der Zertifikate, die für den Aufbau der VPN-Kanäle verwendet werden. Die erforderlichen Informationen zur Prüfung der Gerätezertifikate werden dem EVG in Form einer (signierten) Trust-service Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch mittels der aktuell gültigen TSL und CRL (siehe FPT_TDC.1/NK.Zert).

7.1.4. NK.Stateful Packet Inspection

Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“ (engl. „stateful packet inspection“ oder auch „stateful inspection“ genannt). Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird.

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

7.1.5. NK.Selbstschutz

Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren. Versuche, den ausführbaren Code zu verändern werden durch Prüfung der Integrität der installierten SW Images bei jedem Start (Secure Boot) gewährleistet (siehe Selbsttests).

Speicheraufbereitung

Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben mit Nullen (siehe FDP_RIP.1/NK). Der EVG speichert medizinische Daten nicht dauerhaft. Ausnahmen sind die Speicherung von Daten während ihrer Ver- und Entschlüsselung; auch diese werden sobald wie möglich nach ihrer Verwendung gelöscht.

Selbsttests

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

Damit ist auch die Integrität der Implementierung kryptographischer Verfahren sichergestellt. Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K als Seed Quelle für den Zufallszahlengenerator des Betriebssystems. Dieser ist durch die Prüfung der Integrität ebenfalls vor Manipulationen abgesichert. Der Benutzer kann die Selbsttests durch Neustart des EVGs selbst anstoßen. Schlägt die Prüfung der Integrität fehl, so wird ein Neustart des EVG durchgeführt. Dies führt dann bei manipulierten Komponenten zu einem „Endless Loop“

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

Schutz von Geheimnissen, Seitenkanalresistenz

Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme einschließlich der Kenntnisnahme nach Angriffen durch Seitenkanal-Analysen (side channel analysis), siehe FPT_EMS.1/NK. Dies gilt grundsätzlich für *kryptographisches Schlüsselmaterial* (siehe Tabelle 4: Sekundäre Werte in Abschnitt 3.1.1.1).

Der private Authentisierungsschlüssel für das VPN wird bereits durch das gSMC-K und dessen Resistenz gegen Seitenkanalangriffe geschützt. Der EVG verhindert darüber hinaus den Abfluss von geheimen Informationen wirkungsvoll, etwa die Session Keys der VPN-Verbindung oder zu schützende Daten der TI und der Bestandsnetze.

Sicherheits-Log

Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation [27], Abschnitt 4.1.10 wie unter Sicherheitsdienst *Protokollierung* in Abschnitt 1.3.5 beschrieben. Diese Funktionalität ist mit FAU_GEN.1/NK.SecLog und FAU_GEN.2/NK.SecLog modelliert.

7.1.6. NK.Administration

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

Der EVG verwaltet eine Administrator-Rolle (FMT_SMR.1./NK). Der Administrator muss autorisiert sein (FIA_UID.1/NK.SMR, FMT_SMR.1./NK und FIA_UAU.1/NK.SMR), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1/NK). Die Authentisierung erfolgt dabei durch den Netzkonnektor selbst, siehe O.NK.Admin_Auth.

Die Wartung selbst erfolgt unter der Annahme, dass der Administrator über Netzwerkverbindungen (z. B. LAN, WAN) zugreift, stets über eine sichere TLS Verbindung (siehe FTP_TRP.1/NK.Admin bzw. FTP_ITC.1/NK.TLS).

Die administrativen Tätigkeiten bzw. Wartungstätigkeiten werden in FMT_SMF.1/NK aufgelistet. Dazu gehören die Verwaltung der Filterregeln für den dynamischen Paketfilter sowie das Aktivieren und Deaktivieren des VPN-Tunnels.

Die Administration der Filterregeln für den dynamischen Paketfilter (siehe: FDP_IFC.1/NK.PF) ist den Administratoren vorbehalten (FMT_MSA.1/NK.PF).

Software Update

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

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

Im Falle einer Software-Aktualisierung wird der EVG neu gestartet und dieselbe Bootchain wie in der Sicherheitsfunktion „NK.Selbstschutz“ beschrieben abgelaufen, aber vom Bootloader wird das neue Update-Paket auf Integrität geprüft und bei erfolgreicher Prüfung geladen. Das alte Image wird vom EVG verworfen. Schlägt die Prüfung der Integrität fehl, so wird das Update-Paket verworfen und ein Neustart des EVG durchgeführt mit dem das ursprüngliche SW Image geladen wird. Durch die Prüfung des Update-Pakets analog zum regulären Boot Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können (FDP_UIT.1/NK.Update).

7.1.7. NK.Kryptographische Basisdienste

Der Konnektor implementiert gemäß der Vorgaben des Dokuments „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt]“ [30] die im Folgenden aufgelistete kryptographischen Primitive.

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

Die kryptographischen Basisdienste (z.B. Hash-Berechnung, AES Ver-/Entschlüsselung) des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des VPN Kanals).

7.1.8. NK.TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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

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

Die kryptographischen Basisdienste für TLS (z.B. HMAC-Berechnung, AES Ver-/Entschlüsselung) des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des TLS Kanals).

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

Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen werden X.509 Zertifikate verwendet. Entsprechende Zertifikate für die Kommunikation mit

Clientsystemen können vom EVG erzeugt werden (FCS_CKM.1/NK.Zert). Der EVG bietet dem Administrator eine sichere Schnittstelle zum exportieren dieser X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel (FDP_ETC.2/NK.TLS). Bei Zertifikaten für Serversysteme werden die zugehörigen privaten Schlüssel nicht exportiert. Zertifikate für die Kommunikation mit Clientsystemen können auch vom EVG gemäß FDP_ITC.2/NK.TLS über die gesicherte Management-Schnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Die importierten Zertifikate werden ebenfalls nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.

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

7.2. Sicherheitsfunktionen des Anwendungskonnektors

Die funktionalen Sicherheitsanforderungen werden im Folgenden nach funktionalen Gruppen gegliedert. Die funktionalen Gruppen orientieren sich an den in Abschnitt 6.3 beschriebenen Sicherheitsanforderungen, insbesondere der in Kapitel 6.3.3 definierten Dienste (hier nur kurz in Stichworten rekapituliert):

- AK.Identifikation und Authentisierung: Der Konnektor setzt unterschiedliche Mechanismen zur Identifikation und Authentisierung von Benutzern um.
- AK.Zugriffskontrolldienst: Durch den Zugriffskontrolldienst wird eine Prüfung auf Zugriffsberechtigung für die angeforderten Ressourcen durchgeführt.
- AK.Kartenterminaldienst: Der Kartenterminaldienst managt alle vom Konnektor adressierbaren Kartenterminals.
- AK.Chipkartendienst: Der Chipkartendienst managt alle in den angeschlossenen Kartenterminals gesteckten Karten.
- AK.Signaturdienst: Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten und Prüfen von Dokumentensignaturen.
- AK.Software-Update: Der Konnektor ermöglicht das Einspielen von Software Updates
- AK.Verschlüsselungsdienst: Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an
- AK.TLS-Kanäle: Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung. Die Verwaltung von TLS-Kanälen wird durch den Anwendungskonnektor durchgeführt.
- AK.Sicherer Datenspeicher: Der Konnektor stellt ein Datenspeicher zur Verfügung, in welchem der alle sicherheitskritischen, veränderlichen Daten dauerhaft speichert werden, die für seinen Betrieb relevant sind
- AK.Fachmodul VSDM: Das Versicherten Stammdaten Management Fachmodul ermöglicht es Versichertenstammdaten der eGK zu verwalten.
- AK.Sicherheitsmanagement: Über die Managementschnittstelle kann der Konnektor administriert werden.

- AK.Schutz der TSF: Der Konnektor setzt verschiedene Mechanismen zum Schutz der TSF um.
- AK.Sicherheitsprotokollierung: Der Konnektor führt eine Protokollierung im Sicherheits-Log.

7.2.1. AK.Identifikation und Authentisierung

Der Konnektor setzt unterschiedliche Mechanismen zur Identifikation und Authentisierung von Benutzern um (FIA_UAU.5/AK). Funktionalität des Konnektors die vor der Identifikation und Authentisierung von Benutzern ausgeführt werden kann ist sind in FIA_UAU.1/AK und FIA_UID.1/AK definiert

Die Management-Schnittstelle des Konnektors durch Passworteingabe vor unautorisiertem Zugriff geschützt (FIA_SOS.1/AK.Passwörter) Die folgenden Anforderungen nach [27], TIP1-A_4808 werden vom Konnektor an die Administrator Passwörter gestellt:

Für die Passworterstellung setzt der Konnektor folgende Anforderungen um:

- dem Benutzer ist es möglich sein, die Zeichen eines Passworts aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern zu wählen. Ein Passwort muss Zeichen aus mindestens drei dieser Zeichenklassen enthalten.
- ein Passwort muss mindestens 8 Zeichen lang sein
- ein Passwort darf nicht die zugehörige Benutzerkennung enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung)
- die Wiederholung alter Passwörter beim Passwortwechsel durch den Benutzer selbst wird vom Konnektor verhindert (Passworthistorie). Dazu erkennt der Konnektor die letzten drei Passwörter eines Benutzers bei der Passwortneuvergabe und lehnt diese als neues Passwort ab.

Für die Passwortverarbeitung setzt der Konnektor folgende Anforderungen um:

- für die Erstanmeldung neuer Benutzer werden Einmalpasswörter vergeben, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Gleiches gilt, wenn ein Passwort eines Benutzers vom Super-Admin zurückgesetzt wird.
- jeder Benutzer kann sein eigenes Passwort jederzeit ändern
- bei der Eingabe wird das Passwort nicht im Klartext auf dem Bildschirm angezeigt
- die Passwörter werden im Konnektor zugriffssicher gespeichert
- der Konnektor initiiert nach einem durch den Super-Admin konfigurierbaren Zeitraum (Voreinstellung: 120 Tage) einen Passwortwechsel beim nächsten Login
- erfolglose Anmeldeversuche werden mit einer Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt. Insbesondere wird bei erfolglosen Anmeldeversuchen nicht erkennbar, ob der eingegebene Benutzername oder das eingegebene Passwort (oder beides) falsch ist.
- Nach einer Fehleingabe des Passworts erfolgt eine Verzögerung bis zur nächsten Eingabemöglichkeit des Passworts für dieselbe Benutzerkennung. Die Verzögerung beträgt 3 Sekunden.

Im Rahmen des Pairing eines eHealth Kartenterminals generiert der Konnektor das „pairing secret“ mit hinreichend großer Entropie (FIA_SOS.2/AK.PairG). Wird ein angeschlossenes Kartenterminal für Stapelsignaturen verwendet fordert der Konnektor die Übertragung der DTBS über einen sicheren Kanal der mittels *card-to-card authentication* mit dem HBA ausgehandelt wird (FIA_API.1/AK).

7.2.2. AK.Zugriffsberechtigungsdienst

Der Zugriffsberechtigungsdienst (oder Zugriffskontrolldienst) ist ein interner Dienst des Konnektors der automatisch bei Aufruf einer Operation des Konnektors durch das Clientsystem umgesetzt wird. Durch den Zugriffskontrolldienst wird eine Prüfung auf Zugriffsberechtigung für die angeforderten Ressourcen durchgeführt.

Die erlaubten Zugriffsmöglichkeiten werden über ein Informationsmodell (kurz Infomodell) definiert (FDP_ACC.1/AK.Infomod FDP_ACF.1/AK.Infomod). Durch das Infomodell werden Mandanten definiert und Clientsysteme sowie die vom Konnektor verwalteten externen Ressourcen (Kartenterminal mit Slots, Arbeitsplatz, SMC-Bs) zugeordnet. Die entsprechenden Zuordnungen werden durch einen Administrator eingestellt (FMT_MSA.3/AK.Infomod, FMT_MSA.1/AK.Infomod) und beinhalten die erlaubten Zugriffswege vom Clientsystem über Arbeitsplatz zum Kartenterminal und dessen Slots.

7.2.3. AK.Kartenterminaldienst

Die Aufgabe des Kartenterminaldienstes ist das Management aller vom Konnektor adressierbaren Kartenterminals. Dabei kapselt der Kartenterminaldienst die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule (FDP_ACC.1/AK.eHKT, FDP_ACF.1/AK.eHKT). Über den Kartenterminaldienst können TLS Kanale zu den KTs auf und abgebaut werden sowie SICCT-Kommandos gesendet und empfangen werden.

Der Anwendungskonnektor kommuniziert mit den konfigurierten eHealth-Kartenterminals über TLS-Kanäle (FDP_UCT.1/AK.TLS, FDP_UIT.1/AK.TLS). Der Netzkonnektor stellt diese Kommunikationskanäle kontrolliert dem Anwendungskonnektor zur Verfügung.

Informationen über die Arbeitsplatzkonfiguration eines angeschlossenen Kartenterminals können vom Kartenterminaldienst ausgegeben werden (FMT_MTD.1/AK.eHKT_Abf) Nur der Administrator darf diese Daten auch verändern(FMT_MTD.1/AK.eHKT_Mod).

7.2.4. AK.Kartendienst

Die eHealth-Kartenterminals unter der Steuerung des Anwendungskonnektors können verschiedene Chipkarten, KVK, eGK, SMC-B und HBA aufnehmen. Die in den eHealth-Kartenterminals eines Arbeitsplatzes gesteckten Chipkarten mit ihren logischen Kanälen bilden einen dynamischen Kontext (s. [27]). Die Identifikation dieser Chipkarten erfolgt durch Kartenhandles. Der EVG stellt Sicherheitsfunktionen des Chipkartendienstes anderen Diensten, dem Clientsystembereit oder Fachmodulen bereit (FDP_ACC.1/AK.KD). Dazu gehören der Aufbau und die Verwaltung logischer Kanäle und die Kommunikation mit der Karte via Chipkartenkommandos. Der Chipkartendienst regelt dabei den Zugriff auf die Chipkarten für die verschiedenen Dienste und Anwender (FDP_ACF.1/AK.KD). Zudem wird durch den Chipkartendienst die lokale und entfernet PIN Eingabe an den Kartenterminals umgesetzt (FDP_ACC.1/AK.PIN) und die unterschiedlichen Anforderungen an lokale und entfernet PIN

Eingabe und der damit verbundene Umgang mit den Authentisierungsverifikationsdaten (VAD) geregelt (FDP_ACF.1/AK.PIN). In FMT_MSA.4/AK werden übergreifende Anforderungen an den Chipkartendienst definiert.

Daten einer eGK werden nicht über den Steckzyklus der Karte hinaus im EVG gespeichert. Daten von HBA und SM-B werden nicht länger als 24 Stunden im EVG zwischengespeichert. Dabei werden sensitive Daten mit konstanten oder zufälligen Werten überschrieben, sobald sie nicht mehr verwendet werden (FDP_RIP.1/AK)

7.2.5. AK.Signaturdienst

Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten (FDP_ACC.1/AK.Sgen, FDP_ACF.1/AK.Sgen) und Prüfen von Dokumentensignaturen (FDP_ACC.1/AK.SigPr, FDP_ACF.1/AK.SigPr). Die zu signierenden oder zu prüfenden Daten werden vom Konnektor entsprechend der referenzierten Signaturrichtlinie behandelt. Dabei wird bei Import dieser Daten die angegebene Signaturrichtlinie auf Zulässigkeit geprüft (FDP_ITC.2/AK.Sig, FMT_MSA.3/AK.Sig). Die Plattform des Konnektors stellt selbst keine Signaturrichtlinien bereit. Das unterstützte Fachmodul NFDM bringt eine entsprechende Signaturrichtlinie in den Konnektor ein. In FMT_MSA.4/AK werden übergreifende Anforderungen an den Signaturdienst definiert.

Der Signaturdienst umfasst die Funktionalität der nicht-qualifizierten elektronischen Signatur (nonQES) gemäß gültiger Signaturrichtlinie mit Hilfe der vom Chipkartendienst verwalteten Chipkarten. (FDP_DAU.2/AK.Sig). Zudem können qualifizierte elektronische Signaturen (QES) mit Hilfe der qualifizierten Signaturerstellungseinheit (QSEE) erzeugt werden (FDP_DAU.2/AK.QES). Der HBA (bzw. HBA-Vorläuferkarten) als Teil der QSEE wird vom Chipkartendienst verwalteten. Die zu signierenden Daten werden vom Konnektor an die entsprechende Chipkarte übertragen (FTP_ITC.1/AK.QSEE). Veränderungen an den zu signierenden Daten ab der Übergabe durch den EVG bei Aufruf des Signierdienstes bis zur Rückgabe der signierten Daten an den EVG können durch eine Gegenprüfung der erhaltenen Signatur durch den EVG festgestellt werden (FDP_SDI.2/AK).

Der EVG unterstützt die „Komfortsignatur“. Diese Funktionalität wird wie folgt umgesetzt (A_19102-04 und A_19103-06):

Wenn die Komfortsignatur für eine HBA-Kartensitzung aktiviert ist (SAK_COMFORT_SIGNATURE=enabled und Komfortsignatur-Modus aktiv) , wird der Authentisierungssatus der HBA-Kartensitzung erst dann zurückgesetzt, wenn eine konfigurierte Anzahl an einzelnen Signaturoperation durchgeführt wurde (SAK_COMFORT_SIGNATURE_MAX, Default=100, A_19100) oder ein konfigurierter Zeitwert abgelaufen ist (SAK_COMFORT_SIGNATURE_TIMER, Default=6h, A_18686-01).

Die Konfigurationswerte für das Aktivieren der Komfortsignatur-Funktionalität, für den Timer und für den Zähler können nur vom Administrator verwaltet werden (TIP1-A_4680-03). Zudem wird der Authentisierungssatus aller HBAs bzw. HBA-Kartensitzungen bei Deaktivierung durch die Operation DeactiveComfortSignature oder direkt durch Deaktivierung des Komfortsignatur-Modus in der Managementoberfläche (SAK_COMFORT_SIGNATURE=disabled) zurückgesetzt.

Zudem wird bei Aktivierung der Komfortsignatur die übermittelte UserID auf Eindeutigkeit in Bezug auf die letzten 1000 Aufrufe (A_20074) und auf korrekte Länge (128 Bit) und Format

RFC4122 geprüft (A_20073-01). Diese UserID ist als Authentisierungsgeheimnis zu behandeln und wird nicht vom Konnektor ausgegeben. Der TOE setzt entsprechend FDP_ACF.1.2/AK.Infomod (TIP1-A_4524-02) durch die Prüfung des Aufrufkontext durch, dass nur der Nutzer Komfortsignatur-Aufträge auslösen kann (SignDocument und TUC_KON_170), der die selbe UserID präsentiert, wie diese beim Aktivieren des Komfortsignatur-Modus für diese HBA-Kartensitzung (ActivateComfortSignature) präsentiert wurde. Schlägt die Prüfung fehl, wird die Operation abgebrochen. Die eigentliche Authentifizierung des Nutzers beim Auslösen der Komfortsignatur erfolgt außerhalb des TOE im Clientsystem. Es erfolgt ein entsprechender Hinweis im Handbuch bezüglich der Notwendigkeit und Bedeutung der Nutzer-Authentisierung, A_19101.

Der Signaturdienst unterstützt die folgenden Signaturformate für nonQES und QES:

- XAdES für XML Dokumente (Nur QES mit NFDM-Signaturrichtlinie),
- CAdES für XML, PDF/A, Text und TIFF Dokumente
- PAdES für PDF/A Dokumente.

Darüber hinaus wird für nonQES das folgende Signaturformat unterstützt

- CAdES für Binärdokumente

Zudem wird für nonQES und QES PKCS#1 ECDSA, RSASSA-PSS und RSASSA-PKCS1-v.5 unterstützt.

Das Prüfen von Dokumentensignaturen erfolgt anhand von Zertifikaten (FDP_DAU.2/AK.Cert). Bei Feststellung ungültig erzeugter Signaturen wird der Benutzer entsprechend durch eine Warnmeldung benachrichtigt (FTA_TAB.1/AK.SP)

Der Benutzer des Clientsystems muss seine Signatur-PIN an einem Kartenterminal eingeben. Über das Clientsystem wird die gültige Signaturrichtlinie für zu signierende Daten und der angegebener Zeitpunkt signierter Daten für die Signaturprüfung über die Aufruf-Parameter der Entsprechenden Operationen an der Schnittstelle des EVG übergeben (FMT_MSA.1/AK.User)

Der Konnektor generiert bei bestimmten PIN-Verifikationen vor der Aufforderung zur PIN-Eingabe an einem eHealth-Kartenterminal eine eindeutige sechsstellige Jobnummer (FIA_SOS.2/AK.Jobnummer), welche den Auftrag kennzeichnet, für dessen Verarbeitung die PIN-Eingabe erfolgen soll. Diese Jobnummer wird vom Konnektor im Display des eHealth-Kartenterminals neben der PIN-Eingabeaufforderung angezeigt (FTA_TAB.1/AK.Jobnummer).

Im Folgenden werden die für Signatur-Erstellung und Verifikation verwendeten Algorithmen angegeben:

Erzeugung der DTBS:

- SHA-256, SHA-384 und SHA-512 (FCS_COP.1/AK.SHA)

Signatur Verifikation:

- RSASSA-PKCS1-v1_5 signature verification mit 1976 Bit bis 4096 Bit (FCS_COP.1/AK.SigVer.SSA)
- RSASSA-PSS signature verification 1976 Bit bis 4096 Bit (FCS_COP.1/AK.SigVer.PSS)

- ECDSA mit 256 bit (FCS_COP.1/AK.SigVer.ECDSA)

Erzeugung von Dokumenten-Signaturen:

- XAdES with SHA-256 (FCS_COP.1/AK.XML.Sign)
- CAdES with SHA-256 (FCS_COP.1/AK.CMS.Sign)
- PAdES (PDF/A) with SHA-256 (FCS_COP.1/AK.PDF.Sign)

Dokumentensignaturen werden mit Unterstützung der Signatur Smartcards (z.B. HBA) erzeugt. Die DTBS wird mit SHA-256 vom EVG erzeugt. Die Signaturberechnung wird von der Signaturkarte durch RSA mit PKCS#1v2.2 PSS erzeugt.

Verifikation von Dokumenten-Signaturen:

- XAdES (FCS_COP.1/AK.XML.SigPr)
- CAdES (FCS_COP.1/AK.CMS.SigPr)
- PAdES (FCS_COP.1/AK.PDF.SigPr

jeweils mit

- SHA-256, SHA-384 oder SHA-512 für RSASSA-PKCS1-v1_5 oder RSASSA-PSS mit1976 Bit bis 4096 Bit Schlüssellänge
- SHA-256 für ECDSA mit 256 Bit Schlüssellänge

Geheime Kryptographische Schlüssel, zu signierende Daten und signierte Daten werden nach Verwendung durch den Konnektor unzugänglich gemacht (FDP_RIP.1/AK)

7.2.6. AK.Software-Update

Signierte Update-Pakete werden importiert und im Datenspeicher des EVG abgelegt. Sobald ein Update-Paket zur Verfügung steht signalisiert der TOE das ein Software Update zur Verfügung steht. Der Administrator kann die Version des Update-Paketes prüfen und den Updateprozess anstoßen (FDP_ACC.1/AK.Update). Automatische Installation von Software Updates wird vom EVG unterstützt. Zudem dürfen von Anwendungskonnektor und Netzkonnektor nur Update-Pakete übernommen werden, deren Signatur erfolgreich geprüft wurde. Die Firmwaregruppe des Updates muss gleich oder höher der gegenwärtig installierten Firmwaregruppe sein (FDP_ACF.1/AK.Update).

Der Updateprozess verhindert, dass manipulierte Update-Pakete eingespielt werden können (FDP_UIT.1/AK.Update), siehe auch „Software Update“ in Kapitel 7.1.6.

Fachmodule können nur im Rahmen von Software-Updates des Konnektors aktualisiert oder eingebracht werden.

7.2.7. AK.Verschlüsselungsdienst

Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver- und Entschlüsseln von Dokumenten an (FDP_ACC.1/AK.Enc, FDP_ACF.1/AK.Enc). In

FMT_MSA.4/AK werden übergreifende Anforderungen an den Verschlüsselungsdienst definiert.

Der Verschlüsselungsdienst bietet für XML, PDF/A, Text, TIFF und Binärdaten die hybride Ver- /Entschlüsselung nach dem CMS Standard [RFC5652] bzw. die symmetrische Ver-/Entschlüsselung mittels AES-GCM an. Zudem wird für XML-Dokumente die hybride Ver-/Entschlüsselung nach [XMLEnc] unterstützt.

Dem Konnektor werden durch das Clientsystem die zu verschlüsselnden und zu entschlüsselnden Dokumente übergeben, die zu verwendende Verschlüsselungsrichtlinie durch den Fachdienst bzw. den Anwendungsfall identifiziert und beim Verschlüsseln eines Dokuments die vorgeschlagenen Empfänger des Dokuments angegeben. Vor dem Verschlüsseln eines Dokuments wird die Gültigkeit der zu benutzenden Verschlüsselungszertifikate geprüft. (FDP_ITC.2/AK.Enc, FDP_ETC.2/AK.Enc).

Im Folgenden werden die für die Ver- und Entschlüsselung verwendeten Algorithmen angegeben:

Symmetrische Ver- und Entschlüsselung:

- AES-GCM mit 128 bit, 192 bit and 256 bit (FCS_COP.1/AK.AES)

Hybride Ver- und Entschlüsselung:

- XML-Dokumente: RSAOAEP mit 2048 Bit Schlüssellänge oder ECIES mit 256 Bit Schlüssellänge und AES-GCM mit 128 Bit, 192 Bit und 256 Bit Schlüssellänge und 128 Bit GMAC (FCS_COP.1/AK.XML.Ver, FCS_COP.1/AK.XML.Ent)
- XML, PDF/A, Text, TIFF und Binärdaten: RSAOAEP mit 2048 Bit Schlüssellänge oder ECIES mit 256 Bit Schlüssellänge und AES-GCM mit 128 Bit, 192 Bit und 256 Bit Schlüssellänge und 128 Bit (FCS_COP.1/AK.CMS.Ver, FCS_COP.1/AK.CMS.Ent)

Dabei wird die hybride Verschlüsselung auf AES-GCM mit 256 Bit Schlüssellänge beschränkt. Für die Entschlüsselung wird AES-GCM mit 128 Bit, 192 Bit und 256 Bit Schlüssellänge unterstützt.

Der EVG erzeugt die AES Schlüssel (FCS_CKM.1/AK.AES) und löscht diese nach Verwendung sicher (FCS_CKM.4/AK).

Geheime Kryptographische Schlüssel, zu verschlüsselnde Daten, verschlüsselte Daten, vorgeschlagene Empfänger und entschlüsselte Daten werden nach Verwendung durch den Konnektor unzugänglich gemacht (FDP_RIP.1/AK)

7.2.8. AK.TLS-Kanäle

Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung, siehe 7.1.8 NK.TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen. Die Verwaltung von TLS-Kanälen wird duch den Anwendungskonnektor durchgeführt.

Der Anwendungskonnektor initiiert dabei entsprechende der Vorgaben in Tabelle 24 den Auf- und Abbau der TLS-Kanäle und stellt den Endpunkt für das Senden und Empfangen der Nutzdaten dar (FDP_ACC.1/AK.TLS, FDP_ACF.1/AK.TLS). Für das VSDM Fachmodul wird zudem TLS Session Resumption unterstützt.

Der Administrator kann konfigurieren, ob für Verbindungen zum Clientsystem TLS-Kanäle verwendet werden müssen (ANCL_TLS_MANDATORY, ANCL_CAUT_MANDATORY) und einen Zertifikatsbasierten oder Passwortbasierten Authentisierungsmechanismus (ANCL_CAUT_MODE) festlegen. (FMT_MSA.1/AK.TLS, FMT_MSA.3/AK.TLS). Für den Dienstverzeichnisdienst kann die explizit die verpflichtende Nutzung von TLS deaktiviert werden (ANCL_DVD_OPEN).

TLS Kanäle werden für die Kommunikation mit Fachdiensten (FTP_ITC.1/AK.FD), mit dem zentralen Verzeichnisdienst (FTP_ITC.1/AK.VZD), dem KSR (FTP_ITC.1/AK.KSR), dem TSL-Dienst (FTP_ITC.1/AK.TSL), bei ANCL_TLS_MANDATORY = Enabled mit den Clientsystemen im LAN (FTP_ITC.1/AK.CS) und mit den angebundene eHealth Kartenterminals (FTP_ITC.1/AK.eHKT) verwendet.

Benutzerdaten, die über den TLS-Kanal zwischen EVG und eHealth-Kartenterminals übermittelt wurden, werden nach Verwendung durch den Konnektor unzugänglich gemacht (FDP_RIP.1/AK).

7.2.9. AK.Sicherer Datenspeicher

Der Konnektor stellt einen Datenspeicher zur Verfügung, in welchem er alle sicherheitskritischen, veränderlichen Daten dauerhaft speichert, die für seinen Betrieb relevant sind (FDP_ACC.1/AK.SDS, FDP_ACF.1/AK.SDS). Dieser Datenspeicher sichert die Integrität, Authentizität und Vertraulichkeit der in ihm hinterlegten Daten bzw. der aus ihm entnommenen Daten. Der Konnektor stellt den in ihm laufenden Fachmodulen ebenfalls eine Nutzung dieses Datenspeichers für ihre sensiblen Daten zur Verfügung.

Es werden keine Datenobjekte mit dem Sicherheitsattribut „Administratorobjekt“ verwaltet.

7.2.10. AK.Fachmodul VSDM

Das Versicherten Stammdaten Management (VSDM) Fachmodul ist fester Bestandteil des EVGs und ermöglicht es, Versichertenstammdaten einer eGK zu lesen, zu schreiben oder um neue Einträge zu ergänzen (FDP_ACC.1/AK.VSDM, FDP_ACF.1/AK.VSDM). Die eGK wird dabei über AK.Kartenterminaldienst und AK.Kartendienst angesprochen. Das VSDM Fachmodul kann über die Management-Oberfläche administriert werden (FMT_MSA.1/AK.VSDM, FMT_MSA.3/AK.VSDM).

7.2.11. AK.Sicherheitsmanagement

Der Konnektor verwaltet verschiedene Rollen, wie Administrator, Clientsystem, Kartenterminals und Chipkarten (FMT_SMR.1/AK). Auf die Management Schnittstelle hat nur ein autorisierter Administrator Zugriff. Dieser kann zum Beispiel Kartenterminals managen, Arbeitsplätze konfigurieren, Sicherheitsrichtlinien und TLS-Kanäle verwalten (FMT_SMF.1/AK). Dazu gehört auch das Verwalten von Software Updates für EVG und

angebundene Kartenterminals, Verwalten von Zertifikaten und Durchführen eines Werksreset (FMT_MTD.1/AK.Admin). Insbesondere kann der Administrator die Online-Anbindung des Konnektors im Netz des Leistungserbringers konfigurieren (MGM_LU_ONLINE) und die QES Funktionalität des Signaturdienst de- und aktivieren (MGM_LU_SAK), (FMT_MOF.1/AK). Über die öffentlichen Schlüssel der CVC root CA sind in der gSMC-K gespeichert und können nur durch das CMS System der gSMC-K gelöscht werden. Über cross CVC Zertifikate können durch den Anwendungskonnektor aber weitere öffentlichen Schlüssel der CVC root CA eingebracht werden (FMT_MTD.1/AK.Zert).

7.2.12. AK.Schutz der TSF

Der Konnektor kann die für QES und nonQES benötigten Zertifikate interpretieren, sowie Verschlüsselungszertifikat und CV-Zertifikate. Zudem werden Information gültiger TSL und CRL Listen in die Prüfungen einbezogen sowie BNetzA-VL bzw. die entsprechenden Hashwerte (FPT_TDC.1/AK). Die Zulässigkeit importierter zu signierenden bzw. zu prüfender signierten Daten wird gemäß implementierten Signaturrichtlinien geprüft. Durch das Fachmodul NFDM wird eine entsprechende Signaturrichtlinie in den Konnektor eingebracht.

Der Konnektor setzt die in [gemSpec_Kon], TAB_KON_503 definierten Fehlbetriebszustände um (Error Condition). Wird ein sicherheitsrelevanter Betriebszustand erreicht, schränkt der Konnektor seine Funktionalität gemäß [gemSpec_Kon], TAB_KON_504 ein (FPT_FLS.1/AK).

Vor der regulären Kommunikation mit einem eHealth Kartenterminal wird geprüft, ob dieses gepairt ist und im Infomodell des Konnektors korrekt zugeordnet wurde. Ebenso werden gesteckte Chipkarten identifiziert und auf Gültigkeit geprüft. Bei entfernter PIN-Eingabe wird geprüft ob Kartenterminal und HBA für diesen Verwendungsfall zugelassen sind (FPT_TEE.1/AK),

Der Konnektor führt beim Anlauf und regelmäßig während des Normalbetriebs Selbsttests durch (FPT_TST.1/AK.Run-Time), siehe dazu auch „Selbsttests“ in 7.1.5 NK.Selbstschutz. Neben Selbsttests im Rahmen des sicheren Start-Up Prozesse wird insbesondere auch die Implementierung der Trusted Channels (VPN und TLS) beim Hochfahren getestet. Im Normalbetrieb wird regelmäßig der AES und TLS (wie beschrieben in FPT_TST.1/AK.Run-Time) getestet. Durch den sicheren Start-Up Prozesse wird die Integrität des TOEs auf einen sicheren Vertrauensanker im BIOS zurückgeführt. Durch Neustart des Konnektors können die damit verbundenen Prüfungen durch einen Benutzer jederzeit wiederholt werden (FPT_TST.1/AK.Out-Of-Band).

Die vom Anwendungskonnektor erzeugten Protokolleinträge des Sicherheitsprotokolls werden mit einem zuverlässigen Zeitstempel versehen (FPT_STM.1/AK). Der Anwendungskonnektor greift dabei auf die Echtzeituhr zurück, die in regelmäßigen Abständen und auf Anforderung des Administrators vom Netzkonnektor mit einem vertrauenswürdigen Zeitdienst synchronisiert wird, siehe auch „Zeitsynchronisation“ in 7.1.3 NK.Netzdienste.

7.2.13. AK.Sicherheitsprotokollierung

Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation [27], Abschnitt 4.1.10, siehe auch „Sicherheits-Log“ in 7.1.5 NK.Selbstschutz. Diese Funktionalität wird vom

Anwendungskonnektor mit FAU_GEN.1/AK umgesetzt. Nur der Administrator kann Protokolleinträge einsehen (FAU_SAR.1/AK). Protokolleinträge können nicht verändert werden und nicht explizit gelöscht werden (FAU_STG.1/AK). Ältere Einträge werden rollierend überschrieben (FAU_STG.4/AK).

7.3. Sicherheitsfunktionen für die ePA Fachanwendung (PTV4)

7.3.1. VAU-Kanal

In O.AK.VAUSGD wird gefordert: *„Der EVG bietet eine gesicherte Kommunikationsverbindung mittels „VAU-Protokoll“ in die VAU-Instanz des ePA-Aktensystems […], sodass das Abhören von Daten für diese Kommunikation unterbunden ist.“.* Genau dies leistet FTP_ITC.1/VAU. Um diesen Trusted Channel sicher aufzubauen, werden Schlüssel von FCS_CKM.1/VAU erzeugt. Die SFR FCS_COP.1/VAU.AES übernimmt die Inhaltsdatenverschlüsselung und FCS_COP.1/VAU.Auth die Authentifikation der Gegenseite für den Kanal. Das SFR FPT_TDC.1/SGDVAU sichert die Authenfizierung mit X.509 Zertifikaten ab. Geheime Schlüssel werden entsprechend FCS_CKM.4/AK gelöscht.

7.3.2. SGD-Kanal

In O.AK.VAUSGD wird gefordert: *„Der EVG bietet eine gesicherte Kommunikationsverbindung […] mittels „SGD-Protokoll“ in das SGD-HSM des Schlüsselgenerierungsdienst an, sodass das Abhören von Daten für diese Kommunikation unterbunden ist.“.* Genau dies leistet FTP_ITC.1/SGD. Der Trusted Channel wird durch die ECIES-Verschlüsselung nach FCS_COP.1/SGD.ECIES umgesetzt. Der öffentliche ECIES-Schlüssel des HSM wird dazu zusammen mit seiner Signatur und dem entsprechenden Zertifikat mittels *GetPublicKey* Operation eingebracht (FDP_ITC.2/SGD). Die Verwendung des Schlüssels ist nur erlaubt, wenn die Prüfung der Signatur und des Zertifikates erfolgreich sind (FDP_ACC.1/SGD, FDP_ACF.1/SGD). FCS_COP.1/SGD.Auth fordert die Authentifikation der Gegenseite für den Kanal. Das SFR FPT_TDC.1/SGDVAU sichert die Authenfizierung mit X.509 Zertifikaten ab. Geheime Schlüssel werden entsprechend FCS_CKM.4/AK gelöscht.

7.4. Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen

Tabelle 31 und Tabelle 32 im folgenden Abschnitt 7.4.1 stellen die Abbildung der Sicherheitfunktionlität auf Sicherheitsanforderungen zunächst tabellarisch im Überblick dar. In Abschnitt 7.4.2 wird die Abbildung erläutert und die Umsetzung der Anforderungen durch die Sicherheitsfunktionalität begründet.

7.4.1. Überblick

Sicherheitsanforderung des Netzkonnektors an den EVG	7.1.1 **NK.VPN-Client**	7.1.2 **NK.Dynamischer Paketfilter**	7.1.3 **NK.Netzdienste**	7.1.4 **NK.Stateful Packet Inspection**	7.1.5 **NK.Selbstschutz**	7.1.6 **NK.Administration**	7.1.7 **NK.Kryptographische Basisdienste**	7.1.8 **NK.TLS-Kanäle unter Nutzung sicherer kryptographischer**
FTP_ITC.1/NK.VPN_TI	X							
FTP_ITC.1/NK.VPN_SIS	X							
FDP_IFC.1/NK.PF		X						
FDP_IFF.1/NK.PF		X		X				
FMT_MSA.3/NK.PF		X						
FMT_MSA.1/NK.PF		X						
FPT_STM.1/NK			X					
FPT_TDC.1/NK.Zert			X					
FDP_RIP.1/NK					X			
FPT_TST.1/NK					X			
FPT_EMS.1/NK					X			
FAU_GEN.1/NK.SecLog					X			
FAU_GEN.2/NK.SecLog					X			
FMT_SMR.1./NK						X		
FMT_MTD.1/NK						X		
FIA_UID.1/NK.SMR						X		
FIA_UAU.1/NK.SMR						X		
FTP_TRP.1/NK.Admin						X		
FMT_SMF.1/NK						X		
FCS_COP.1/NK.Hash							X	
FCS_COP.1/NK.HMAC							X	
FCS_COP.1/NK.Auth							X	
FCS_COP.1/NK.ESP							X	
FCS_COP.1/NK.IPsec							X	
FCS_CKM.1/NK							X	
FCS_CKM.2/NK.IKE							X	
FCS_CKM.4/NK							X	
FDP_ACC.1/NK.Update						X		
FDP_ACF.1/NK.Update						X		
FDP_ITC.1/NK.Update						X		
FDP_UIT.1/NK.Update						X		
FTP_ITC.1/NK.TLS								X
FPT_TDC.1/NK.TLS.Zert								X
FCS_CKM.1/NK.TLS								X
FCS_COP.1/NK.TLS.HMAC								X
FCS_COP.1/NK.TLS.AES								X
FCS_COP.1/NK.TLS.Auth								X

Sicherheitsanforderung des Netzkonnektors an den EVG	7.1.1 **NK.VPN-Client**	7.1.2 **NK.Dynamischer Paketfilter**	7.1.3 **NK.Netzdienste**	7.1.4 **NK.Stateful Packet Inspection**	7.1.5 **NK.Selbstschutz**	7.1.6 **NK.Administration**	7.1.7 **NK.Kryptographische Basisdienste**	7.1.8 **NK.TLS-Kanäle unter Nutzung sicherer kryptographischer**
FCS_CKM.1/NK.Zert								X
FDP_ITC.2/NK.TLS								X
FDP_ETC.2/AK.Enc								X
FMT_MOF.1/NK.TLS								X

Tabelle 31: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen des Netzkonnektors

Sicherheitsanforderung des Anwendungskonnektors an den EVG	7.2.1 **AK.Identifikation und Authentisierung**	7.2.2 **AK.Zugriffsberechtigungsdienst**	7.2.3 **AK.Kartenterminaldienst**	7.2.4 **AK.Kartendienst**	7.2.5 **AK.Signaturdienst**	7.2.6 **AK.Software-Update**	7.2.7 **AK.Verschlüsselungsdienst**	7.2.8 **AK.TLS-Kanäle**	7.2.9 **AK.Sicherer Datenspeicher**	7.2.10 **AK.Fachmodul VSDM**	7.2.11 **AK.Sicherheitsmanagement**	7.2.12 **AK.Schutz der TSF**	7.2.13 **AK.Sicherheitsprotokollierung**
FAU_GEN.1/AK													X
FAU_SAR.1/AK													X
FAU_STG.1/AK													X
FAU_STG.4/AK													X
FCS_CKM.1/AK.AES							X						
FCS_CKM.4/AK							X						
FCS_COP.1/AK.AES							X						
FCS_COP.1/AK.CMS.Ent							X						
FCS_COP.1/AK.CMS.SigPr					X								
FCS_COP.1/AK.CMS.Sign					X								
FCS_COP.1/AK.CMS.Ver							X						
FCS_COP.1/AK.PDF.SigPr					X								
FCS_COP.1/AK.PDF.Sign					X								
FCS_COP.1/AK.SigVer.ECDSA					X								
FCS_COP.1/AK.SigVer.PSS					X								
FCS_COP.1/AK.SigVer.SSA					X								
FCS_COP.1/AK.SHA					X								
Fehler! Verweisquelle konnte nicht gefunden werden.							X						
Fehler! Verweisquelle konnte nicht gefunden werden.							X						

Sicherheitsanforderung des Anwendungskonnektors an den EVG	7.2.1 **AK.Identifikation und Authentisierung**	7.2.2 **AK.Zugriffsberechtigungsdienst**	7.2.3 **AK.Kartenterminaldienst**	7.2.4 **AK.Kartendienst**	7.2.5 **AK.Signaturdienst**	7.2.6 **AK.Software-Update**	7.2.7 **AK.Verschlüsselungsdienst**	7.2.8 **AK.TLS-Kanäle**	7.2.9 **AK.Sicherer Datenspeicher**	7.2.10 **AK.Fachmodul VSDM**	7.2.11 **AK.Sicherheitsmanagement**	7.2.12 **AK.Schutz der TSF**	7.2.13 **AK.Sicherheitsprotokollierung**
FCS_COP.1/AK.XML.Ent							X						
FCS_COP.1/AK.XML.Sign					X								
FCS_COP.1/AK.XML.SigPr					X								
FCS_COP.1/AK.XML.Ver							X						
FDP_ACC.1/AK.eHKT			X										
FDP_ACC.1/AK.Enc							X						
FDP_ACC.1/AK.Infomod		X											
FDP_ACC.1/AK.KD				X									
FDP_ACC.1/AK.PIN				X									
FDP_ACC.1/AK.Sgen					X								
FDP_ACC.1/AK.SigPr					X								
FDP_ACC.1/AK.TLS								X					
FDP_ACC.1/AK.SDS									X				
FDP_ACC.1/AK.Update						X							
FDP_ACC.1/AK.VSDM										X			
FDP_ACF.1/AK.eHKT			X										
FDP_ACF.1/AK.Enc							X						
FDP_ACF.1/AK.Infomod		X											
FDP_ACF.1/AK.KD				X									
FDP_ACF.1/AK.PIN				X									
FDP_ACF.1/AK.Sgen					X								
FDP_ACF.1/AK.SigPr					X								
FDP_ACF.1/AK.TLS								X					
FDP_ACF.1/AK.SDS									X				
FDP_ACF.1/AK.Update						X							
FDP_ACF.1/AK.VSDM										X			
FDP_DAU.2/AK.Cert					X								
FDP_DAU.2/AK.QES					X								
FDP_DAU.2/AK.Sig					X								
FDP_ETC.2/AK.Enc							X						
FDP_ITC.2/AK.Enc							X						
FDP_ITC.2/AK.Sig					X								
FDP_RIP.1/AK				X	X		X	X					
FDP_SDI.2/AK					X								
FDP_UCT.1/AK.TLS			X										

Sicherheitsanforderung des Anwendungskonnektors an den EVG	7.2.1 **AK.Identifikation und Authentisierung**	7.2.2 **AK.Zugriffsberechtigungsdienst**	7.2.3 **AK.Kartenterminaldienst**	7.2.4 **AK.Kartendienst**	7.2.5 **AK.Signaturdienst**	7.2.6 **AK.Software-Update**	7.2.7 **AK.Verschlüsselungsdienst**	7.2.8 **AK.TLS-Kanäle**	7.2.9 **AK.Sicherer Datenspeicher**	7.2.10 **AK.Fachmodul VSDM**	7.2.11 **AK.Sicherheitsmanagement**	7.2.12 **AK.Schutz der TSF**	7.2.13 **AK.Sicherheitsprotokollierung**
FDP_UIT.1/AK.TLS			X										
FDP_UIT.1/AK.Update						X							
FIA_API.1/AK	X												
FIA_SOS.1/AK.Passwörter	X												
FIA_SOS.2/AK.Jobnummer					X								
FIA_SOS.2/AK.PairG	X												
FIA_UAU.1/AK	X												
FIA_UAU.5/AK	X												
FIA_UID.1/AK	X												
FMT_MSA.1/AK.User					X								
FMT_MSA.1/AK.Infomod		X											
FMT_MSA.3/AK.Infomod		X											
FMT_MSA.1/AK.TLS								X					
FMT_MSA.3/AK.TLS								X					
FMT_MSA.1/AK.VSDM										X			
FMT_MSA.3/AK.VSDM										X			
FMT_MSA.3/AK.Sig					X								
FMT_MSA.4/AK				X	X		X						
FMT_MOF.1/AK											X		
FMT_MTD.1/AK.Admin											X		
FMT_MTD.1/AK.Zert											X		
FMT_MTD.1/AK.eHKT_Abf			X										
FMT_MTD.1/AK.eHKT_Mod			X										
FMT_SMF.1/AK											X		
FMT_SMR.1/AK											X		
FPT_FLS.1/AK												X	
FPT_STM.1/AK												X	
FPT_TDC.1/AK												X	
FPT_TEE.1/AK												X	
FPT_TST.1/AK.Out-Of-Band												X	
FPT_TST.1/AK.Run-Time												X	
FTA_TAB.1/AK.Jobnummer					X								
FTA_TAB.1/AK.SP					X								
FTP_ITC.1/AK.CS								X					
FTP_ITC.1/AK.eHKT								X					

Sicherheitsanforderung des Anwendungskonnektors an den EVG	7.2.1 **AK.Identifikation und Authentisierung**	7.2.2 **AK.Zugriffsberechtigungsdienst**	7.2.3 **AK.Kartenterminaldienst**	7.2.4 **AK.Kartendienst**	7.2.5 **AK.Signaturdienst**	7.2.6 **AK.Software-Update**	7.2.7 **AK.Verschlüsselungsdienst**	7.2.8 **AK.TLS-Kanäle**	7.2.9 **AK.Sicherer Datenspeicher**	7.2.10 **AK.Fachmodul VSDM**	7.2.11 **AK.Sicherheitsmanagement**	7.2.12 **AK.Schutz der TSF**	7.2.13 **AK.Sicherheitsprotokollierung**
FTP_ITC.1/AK.FD								X					
FTP_ITC.1/AK.QSEE					X								
FTP_ITC.1/AK.VZD								X					
FTP_ITC.1/AK.KSR								X					
FTP_ITC.1/AK.TSL								X					

Tabelle 32: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen des Anwendungskonnektors

Sicherheitsanforderung für die ePA Fachanwendung an den EVG	7.3.1 **VAU-Kanal**	7.3.2 **SGD-Kanal**
FTP_ITC.1/VAU	X	
FCS_CKM.1/VAU	X	
FCS_COP.1/VAU.AES	X	
FCS_COP.1/VAU.Auth	X	
FTP_ITC.1/SGD		X
FCS_COP.1/SGD.ECIES		X
FCS_COP.1/SGD.Auth		X
FDP_ITC.2/SGD		X
FDP_ACC.1/SGD		X
FDP_ACF.1/SGD		X
FPT_TDC.1/SGDVAU	X	X
FCS_CKM.4/AK	X	X

Tabelle 33: Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen der ePA Fachanwendung

7.4.2. Erfüllung der funktionalen Sicherheitsanforderungen

Wie aus Tabelle 31, Tabelle 32 und Tabelle 33 ersichtlich, wird jede Sicherheitsanforderung gemäß Kapitel 6.2 bzw. 6.3 durch die Sicherheitsfunktionen in Kapitel 7.1, 7.2 oder 7.3 umgesetzt. Die Beschreibung der Sicherheitsfunktionen in den Kapiteln 7.1.1-7.1.8 und 7.2.1-7.2.13 sowie 7.3.1-7.3.2 nutzen direkte Referenzen auf die entsprechenden implementierten Sicherheitsfunktionen in Kapiteln 6.2.1-6.2.8 bzw. orientieren sich an der Unterteilung der Kapitel 6.3.1-6.3.7, Insbesondere werden die Dienste aus Kapitel 6.3.3 als Sicherheitsfunktionen modelliert. Die Sicherheitsfunktionen sind damit direkt aus der Unterteilung der Sicherheitsfunktionen des Gesamtkonnektors im Konnektor PP [16] sowie der Erweiterung zu PTV4 abgeleitet.

8. ST-Erweiterung

8.1. Erweiterungen für PTV3, PTV4 und PTV5

Das Protection Profile BSI-CC-PP-0098 [16], das diesem Security Target zugrunde liegt, erfasst alle Sicherheitsanforderungen, die für PTV2 des Konnektors vorgesehen sind. Der EVG setzt jedoch die Anforderungen nach PTV3, PTV4 und PTV5 um (siehe [28]). Da das Protection Profile [16] nicht alle Inhalte aus [28] abdeckt, wurde das vorliegende ST entsprechend erweitert. Die folgenden Tabellen erfassen diese zusätzlichen Sicherheitseigenschaften und gibt eine Erläuterung, wie diese im vorliegenden Security Target erfasst sind.

Anforderung aus [28**] i.V.m. [**27**]**	**Zusammenfassung der Anforderung**	**Umsetzung im ST**
TIP1-A_4710	Medizinische Daten oder personenbezogene Daten (darunter KVNR, ICCSN und CardHolderName) dürfen nicht in Protokolleinträge geschrieben werden.	In Anwendungshinweis 203: erfasst. *Bereits in BSI-CC-PP-0098 [16] umgesetzt, keine besondere Anpassung in diesem Security Target.*
TIP1-A_5482	Prüfung von CV-Zertifikaten nach dem Schalenmodell	In FPT_TDC.1/AK, Element 1.2, Regel (5), erfasst. *Bereits in BSI-CC-PP-0098 [16] umgesetzt, keine besondere Anpassung in diesem Security Target.*
TIP1-A_5484	Der Konnektor MUSS den Fachmodulen die Möglichkeit bereitstellen, die in den Fachmodulspezifikationen gekennzeichneten Konfigurationsdaten persistent zu speichern, auszulesen und zu löschen. Je Fachmodul muss ein exklusiv durch das Fachmodul nutzbarer Speicherbereich verwendet werden.	Seit Version 1.1 der Technischen Richtlinien für die jeweiligen Fachmodule gibt es keine Sicherheitsanforderung bezüglich der Konfigurationsparameter mehr. Das Speichern, Auslesen und löschen von Daten wird durch die Sicherheitsfunktion **AK.Sicherer Datenspeicher** umgesetzt,
TIP1-A_5486	Aktivieren/Deaktivieren des PIN-Schutzes	*Bereits im BSI-CC-PP-0098 ab Version 1.4 ungesetzt, keine besondere Anpassung in diesem Security Target.*

TIP1-A_5505	Kryptographische Prüfung der XML-Dokumentensignatur gemäß TUC_KON_162	*Siehe* Tabelle 38*, TUC_KON_162*
TIP1-A_5538	Signaturrichtlinien bei QES für XML-Dokumentenformate	In FPT_TDC.1.2/AK (9) wurde die Auswahl „Signaturrichtlinie“ eingeschlossen. Außerdem: Anwendungshinweis 46: und Hinweis darunter.
TIP1-A_6025	Zugang zur TI sperren, wenn Deadline für kritische FW-Updates erreicht ist.	In FPT_FLS.1.1/AK aufgenommen: Im Fehlerfall EC_FW_Not_Valid_Status_Blocked ist gemäß TAB_KON_504 vorzugehen.
TIP1-A_7254	Reaktion auf OCSP-Abfrage beim TLS-Verbindungsaufbau	Bemerkung zu Beginn von Abschnitt 6.3.3.7. Siehe auch die Verweise dort.
TIP1-A_7255	Anzeige von Fachmodulversionen	Siehe Tabelle 39.
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	Siehe Anwendungshinweis 102: und FIA_UAU.5/AK.
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	Der Konnektor authentisiert sich gegenüber dem Remote-Management-System mittels validierten TLS-Zertifikat.
TIP1-A_7279	Authentifizierung des Remote-Administrators	Siehe FIA_UAU.5/AK. Der Remote Administrator muss sich mittels Username und Password Authentifizieren.
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	Refinement von FMT_MTD.1/AK.Admin
GS-A_5484 (gemSpec_PKI)	Aktualisierung der BNetzA-VL	Entspricht TIP1-A_6729 von [27] und war schon in PTV2 der CC-Evaluierung zugerechnet. Umgesetzt in BSI-CC-PP-0098.
A_16203	Nutzbarkeit im Zustand EC_FIREWALL_NOT_RELIABLE	Siehe Anwendungshinweis 198:.
GS-A_5081 (gemSpec_Krypt)	Signaturen von PDF/A-Dokumenten (BSI Hinweise: “Nutzung von SHA-256 statt SHA-1”)	Seit Version 2.4.0 (mit Version 0.8 dieses Dokuments ist 2.11.0 der gemSpec_Krypt aktuell) sieht gemSpec_Krypt an dieser Stelle

		vor, dass mind. SHA-256 verwendet wird. Daher wird kein Anpassungsbedarf gesehen. Der Wegfall von ISO9796-2 DS2 ist bereits in der Version 1.4 des PP durchgeführt.

Tabelle 34: ST-Erweiterung für PTV3

Anforderung aus [28**] i.V.m. [**27**]**	**Zusammenfassung der Anforderung**	**Umsetzung im ST**
A_17225-01	Aufbau einer sicheren Verbindung zur Vertrauenswürdige Ausführungsumgebung (VAU)	Durch O.AK.VAUSGD (Anteil VAU) umgesetzt.
A_17548-01	TSL-Signer-CA Zertifikat sicher speichern (ECC-Migration)	Siehe Anmerkung 10
A_17549-01	TSL-Signer-CA Cross-Zertifikat im kritischen Betriebszustand (ECC-Migration)	Siehe Anmerkung 10
A_17661	Gesicherte Übertragung der Hash-Datei für TSL (ECC-Migration)	Siehe Anmerkung 10 und FDP_ACF.1.2/AK.TLS FTP_ITC.1.3/AK.TSL FPT_TDC.1.1/AK (5)
A_17746	Einsatzbereich und Vorgaben für Ver- und Entschlüsselung (ECC-Migration)	Die kryptographischen SFRs müssen immer den korrekten Algorithmus auswählen, siehe Anmerkung 7.
A_17768	Zertifikate und Schlüssel für Signaturerstellung und Signaturprüfung (QES und nonQES)	Die kryptographischen SFRs müssen immer den korrekten Algorithmus auswählen, siehe Anmerkung 8.
A_17777	sicherheitstechnische Festlegungen zum Abruf von kryptographischen Schlüsseln von einem Schlüsselgenerierungsdienst	Durch O.AK.VAUSGD (Anteil SGD) umgesetzt
A_17837−01	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)	FMT_MTD.1/AK.Zert beschreibt die Nutzung von Cross-Zertifikaten. Das SFR gilt auch für den Vertrauensraum-Wechsel nach ECC-RSA.
A_18001	TUC_KON_075 „Symmetrisch verschlüsseln”	SFR FCS_COP.1/AK.AES beschreibt die symmetrische Verschlüsslung.

A_18002	TUC_KON_076 „Symmetrisch entschlüsseln”	SFR FCS_COP.1/AK.AES beschreibt die symmetrische Entschlüsslung.
TIP1−A_4510−04	Sicherheitskritische Fehlerzustände	Abgedeckt durch FPT_FLS.1/AK und dem folgenden Anwendungshinweis 198:
TIP1−A_4569−02	TUC_KON_021 „PIN entsperren“	Ist durchgesetzt durch FDP_ACF.1/AK.PIN.
TIP1−A_4616−02	TUC_KON_070 „Daten hybrid verschlüsseln”	Schon durch SFRs für hybride Entschlüsselung umgesetzt. ECC wird unterstützt.
TIP1−A_4617−02	TUC_KON_071 „Daten hybrid entschlüsseln“	Schon durch SFRs für hybride Entschlüsselung umgesetzt. ECC wird unterstützt.
TIP1−A_4646−02	ab PTV4: TUC_KON_155 „Dokumente zur Signatur vorbereiten“	Keine Auswirkung auf die ST Version, da schon in PTV3 umgesetzt
TIP1−A_4653−02	ab PTV4: TUC_KON_160 „Dokumente nonQES signieren“	Schon durch SFRs für Signaturerstellung umgesetzt und ECC wird unterstützt.
TIP1−A_4654−03	TUC_KON_161 „nonQES Dokumentsignatur prüfen”	Keine Auswirkung auf die ST Version, da schon in PTV3 umgesetzt
TIP1−A_4672−02	TUC_KON_151 „QES-Dokumentensignatur prüfen“	Keine Auswirkung auf die ST Version, da schon in PTV3 umgesetzt
TIP1−A_4785−03	Konfigurationsparameter VPN-Client	Keine Auswirkung auf die ST Version, da schon in PTV3 umgesetzt
TIP1−A_4832−02	TUC_KON_280 „Konnektoraktualisierung durchführen“	Die SFRs FDP_ACC.1/AK.Update und FDP_ACF.1/AK.Update bilden das Update ab.
TIP1−A_4839−01	Festlegung der durchzuführenden Updates	Die SFRs FDP_ACC.1/AK.Update und FDP_ACF.1/AK.Update bilden das Update ab.
TIP1−A_4840−01	Manuelles Auslösen der durchzuführenden Updates	Die SFRs FDP_ACC.1/AK.Update und FDP_ACF.1/AK.Update bilden das Update ab.
TIP1−A_5540−01	QES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt	Siehe Anwendungshinweis 159:
TIP1−A_5541−01	Referenzen in Dokumenten nicht dynamisch auflösen	Keine Auswirkung auf die ST Version
TIP1−A_5657−02	Freischaltung von Softwareupdates	Die SFRs FDP_ACC.1/AK.Update und FDP_ACF.1/AK.Update bilden

		das manuelle und automatische Update ab.
A_15549	VAU-Client: Kommunikation zwischen VAU-Client und VAU	FTP_ITC.1/VAU setzt die Anforderung um.
A_15561	AES-NI	Siehe Anwendungshinweis 201:
A_16849	VAU-Protokoll: Aktionen bei Protokollabbruch	Durch FCS_CKM.4/AK abgedeckt
A_16852−01	VAU-Protokoll: ECDH durchführen	FTP_ITC.1/VAU gibt explizit die Brainpool Kurve als einzige möglich Kurve an.
A_16883−01	VAU-Protokoll: Aufbau VAUClientHello-Nachricht	FTP_ITC.1/VAU beschreibt die Initierung des VAU Protokols.
A_16884	VAU-Protokoll: Nachrichtentypen und HTTP-Content-Type	FTP_ITC.1/VAU mit Anmerkung 12
A_16900	VAU-Protokoll: Client, Behandlung von Fehlernachrichten	FTP_ITC.1/VAU mit Anmerkung 12 erklärt, dass unter bestimmten Bedingungen die Verbindung abgebrochen wird
A_16903	VAU-Protokoll: Client, Prüfung des VAUClientHelloDataHash-Werts (aus VAUServerHelloData)	FTP_ITC.1/VAU mit Anmerkung 12 erklärt, dass unter bestimmten Bedingungen die Verbindung abgebrochen wird
A_16941−01	VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData	FTP_ITC.1/VAU mit Anmerkung 12 erklärt, dass unter bestimmten Bedingungen die Verbindung abgebrochen wird
A_16943−01	VAU-Protokoll: Schlüsselableitung (HKDF)	FCS_CKM.1/VAU für Schlüsselableitungen/-generierungen
A_16945−02	VAU-Protokoll: Client, verschlüsselte Kommunikation (1)	FTP_ITC.1/VAU mit mit Anmerkung 12
A_16957-01	VAU-Protokoll: Client, verschlüsselte Kommunikation (2)	FTP_ITC.1/VAU mit mit Anmerkung 12
A_17069	VAU-Protokoll: Client Zählerüberlauf	FTP_ITC.1/VAU mit mit Anmerkung 12
A_17070−02	VAU-Protokoll: Aufbau der VAUClientSigFin-Nachricht	FCS_COP.1/VAU.Auth beschreibt die Signaturprüfung mit Anmerkung 12
A_17071	VAU-Protokoll: Versand der VAUClientSigFin-Nachricht	FCS_COP.1/VAU.Auth beschreibt die Signaturprüfung mit Anmerkung 12
A_17074	VAU-Protokoll: Ignorieren von zusätzlichen Datenfeldern in Protokoll-Nachrichten	FTP_ITC.1/VAU mit Anmerkung 12 gibt das an.
A_17081	VAUProtokoll: zu verwendende Signaturschlüssel	FCS_COP.1/VAU.Auth beschreibt die Signaturschlüsselhandhabung

A_17084	VAU-Protokoll: Empfang der VAUServerFin-Nachricht	FTP_ITC.1/VAU mit mit Anmerkung 12
A_17094	TLS-Verbindungen Konnektor (ECC-Migration)	FTP_ITC.1/NK.TLS
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	Siehe Anmerkung 10.
A_17206	XML-Signaturen (ECC-Migration)	FDP_DAU.2/AK.Sig, FDP_DAU.2/AK.QES, FCS_COP.1/AK.XML.SigPr und FCS_COP.1/AK.XML.Sign führen ECDSA als Algorithmus aus.
A_17207	Signaturen binärer Daten (ECC-Migration)	Bereits mit SFRs FCS_COP.1/AK.CMS.Sign und FCS_COP.1/AK.CMS.SigPr umgesetzt
A_17208	Signaturen von PDF/A-Dokumenten (ECC-Migration)	FCS_COP.1/AK.PDF.SigPr und FCS_COP.1/AK.PDF.Sign führen ECDSA als Algorithmus aus.
A_17209	Signaturverfahren für externe Authentisierung (ECC-Migration)	Der Konnektor unterstützt ECDSA FCS_COP.1/AK.SigVer.ECDSA.
A_17210	Konnektor, IKE-Schlüsselaushandlung Fallback (ECC-Migration)	IKE ECC Unterstützung wird in PTV4 nicht umgesetzt.
A_17220	Verschlüsselung binärer Daten (ECIES) (ECC-Migration)	FCS_COP.1/AK.CMS.Ver und FCS_COP.1/AK.CMS.Ent wurden um ECIES erweitert.
A_17221-01	XML-Verschlüsselung (ECIES) (ECC-Migration)	FCS_COP.1/AK.XML.Ent und FCS_COP.1/AK.XML.Ver wurden um ECIES erweitert.
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	FCS_CKM.1/NK.TLS Siehe auch A_17124 in Tabelle 37**.**
A_17359	Signaturen binärer Daten (Dokumente) (ECC-Migration)	Bereits mit FCS_COP.1/AK.CM.SigPr umgesetzt
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	FCS_COP.1/AK.XML.SigPr und FCS_COP.1/AK.XML.Sign führen ECDSA als Algorithmus aus.
A_17874	SGD-Client, Client-authentisiertes ECIES-Schlüsselpaar	FTP_ITC.1/SGD beschreibt die Kurve und die Verwendung von ECDSA.
A_17875	ECIES-verschlüsselter Nachrichtenversand zwischen SGD-Client und SGD-HSM	FTP_ITC.1/SGD, FCS_COP.1/SGD.ECIES, FCS_COP.1/SGD.Auth

		beschreiben die kryptograhischen Verfahren.
A_18004	Vorgaben für die Kodierung von Chiffraten (innerhalb von ePA)	FCS_COP.1/SGD.ECIES mit Anmerkung 18 beschreibt den IV
A_18464	TLS-Verbindungen, nicht Version 1.1	Anwendungshinweis 113: beschreibt, dass TLS Version 1.2 unterstützt wird. Insbesondere werden keine niedrigeren TLS Versionen unterstützt.
A_18467	TLS-Verbindungen, Version 1.3	Version 1.3 wird nicht unterstützt.
A_18624	Konnektor, IPsec/IKE: optionale ECC-Unterstützung	ECC für VPN wird nicht umgesetzt.
GS−A_4376−02	XML-Verschlüsselung – Hybrid, Schlüsseltransport RSAES-OAEP	FCS_COP.1/AK.XML.Ver und der Anwendungshinweis 142: darunter beschreibt diesen Algorithmus.
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	Siehe Anmerkung 10
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	Optionale Anforderung hat keine Auswirkung auf das ST.
A_17821	Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)	Siehe Anmerkung 10
A_17847	Prüfung eines SGD-HSM-Zertifikats (1/2)	FTP_ITC.1/SGD
A_17848	Prüfung eines SGD-HSM-Zertifikats (2/2)	FTP_ITC.1/SGD
A_17888	SGD, KeyDerivation (Client)	Anmerkung 16
A_17892	Aufwärtskompatibilität JSON-Requests und -Responses	FTP_ITC.1/SGD mit der Anmerkung beschreibt das Verhalten
A_17897	SGD-Client, Anfrage GetPublicKey (Client)	Anmerkung 16
A_17899	SGD-Clients, Auswertung der Kodierung des öffentlichen ECIES-Schlüssels eines SGD-HSMs	FTP_ITC.1/SGD mit der Anmerkung 16 beschreibt das Verhalten
A_17900	SGD-Clients, Kodierung des eigenen kurzlebigen ECIES-Schlüssels	FCS_COP.1/SGD.ECIES und Anmerkung 17 erklärt die Schlüsselhandhabung
A_17901	SGD-Clients, Kodierung der Signatur des eigenen ECIES-Schlüssels	FCS_COP.1/SGD.ECIES und Anmerkung 17 erklärt die Schlüsselhandhabung
A_17902	Kontext SGD, Chiffrat-Kodierung beim Nachrichtentransport	FTP_ITC.1/SGD mit der Anmerkung 16 beschreibt die Nachrichten.

A_17903	Kontext SGD, Prüfung der ephemeren ECC-Schlüssel des Senders beim ECIES-Verfahren	FCS_COP.1/SGD.ECIES und Anmerkung 17 beschreibt die Brainpool Kurve
A_17924−01	Anfragen an das SGD-HSM (Client)	FTP_ITC.1/SGD mit der Anmerkung 16 beschreibt dies.
A_17930	interoperables Austauschformat Schlüsselableitungsfunktionalität ePA	FTP_ITC.1/SGD mit der Anmerkung 16 beschreibt dies.
A_18003	SGD-Client, Prüfung der Telematik-ID bei Berechtigungsvergabe	FTP_ITC.1/SGD mit der Anmerkung 16 beschreibt dies.
A_18005	SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars	FTP_ITC.1/SGD
A_18006	SGD-Client, KVNR	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen
A_18024	SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen
A_18025-01	SGD-Client, Anfrage GetAuthenticationToken	FCS_COP.1/SGD.ECIES und die Zufallszahlen werden extern erzeugt
A_18028	SGD-Client, Auswertung der Anfrage GetAuthenticationToken	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen
A_18029	SGD-Client, Anfrage KeyDerivation	FCS_COP.1/SGD.ECIES beschreibt den Algorithmus für die Ableitung
A_18031−01	SGD-Client, Auswertung der Anfrage KeyDerivation	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen
A_18032	SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar	FTP_ITC.1/SGD
A_20478	Zusätzliche Dokumentformate für nonQES-Signatur	Umgesetzt in FCS_COP.1/AK.XML.Sign
A_20977	SGD-Client, Auswertung der Anfrage KeyDerivation	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen

Tabelle 35: ST-Erweiterung für PTV4

Afo-Liste [gemSpec_Kon_KomfSig]	**Zusammenfassung der Anforderung**	**Umsetzung**

A_18686-01	Komfortsignatur-Timer	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 158:
A_19100-01	Komfortsignatur-Zähler	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 158:
A_19101	Handbuch-Hinweis zu Nutzerauthentisierung am Clientsystem bei Komfortsignatur	Siehe Handbuch [110] und Anwendungshinweis 158:
A_19102-04	TUC_KON_158 „Komfortsignaturen erstellen“	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 158: Der Hinweis beschreibt wie die Komfortsignatur funktioniert.
A_19103-06	TUC_KON_170 "Dokumente mit Komfort signieren"	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 158: Der Hinweis beschreibt wie die Komfortsignatur funktioniert.
A_19104−04	TUC_KON_171 „Komfortsignatur einschalten“	FIA_UAU.5/AK, siehe auch Anwendungshinweis 191:
A_19105	TUC_KON_172 „Komfortsignatur ausschalten“	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 191:
A_19258	Secure Messaging bei Komfortsignatur	FIA_UAU.5/AK, FIA_API.1/AK, siehe auch Anwendungshinweis 191:
A_20073-01	Prüfung der Länge der UserId	FIA_UAU.5/AK, siehe auch Anwendungshinweis 158:
A_20074	UserId über 1.000 Vorgänge eindeutig	FIA_UAU.5/AK, siehe auch Anwendungshinweis 158:
TIP1-A_4524-02	TUC_KON_000 „Prüfe Zugriffsberechtigung” Regel R9	Die Regel R9 steht in TAB_KON_514 welche durch FDP_ACF.1.2/AK.Infomod umgesetzt wird.
TIP1−A_4680−03	Konfigurationswerte des Signaturdienstes	FDP_ACF.1/AK.Sgen, siehe auch Anwendungshinweis 158:
A_22344	Mindestens zwei parallele Komfortsignatursessions für einen HBA	FDP_ACF.1/AK.Sgen und Anwendungshinweis 158:

A_22352	Unabhängige Komfortsignatur-Timer bei parallelen Komfortsignatursessions	FDP_ACF.1/AK.Sgen und Anwendungshinweis 158:
A_22459	Unabhängige Komfortsignatur-Zähler bei parallelen Komfortsignatursessions	FDP_ACF.1/AK.Sgen und Anwendungshinweis 158:

Tabelle 36: ST-Erweiterung für PTV5 (Anteil PTV4Plus - Komfortsignatur)

Afo-Liste [gemSpec_Kon] PTV5	**Zusammenfassung der Anforderung**	**Umsetzung**
A_19738	Optionaler Import von Konfigurationsdaten durch lokalen Administrator	**FMT_MTD.1/AK.Admin**
A_19945	Unterstützte Signaturvarianten bei Komfortsignatur	**FDP_DAU.2/AK.QES, FDP_DAU.2/AK.Sig**
TIP1−A_5437−02	Signaturverfahren für externe Authentisierung	Anwendungshinweis 135:
GS−A_5071−01	kryptographische Vorgaben für eine Signaturprüfung in der SAK-Konnektor	6.3.1.3
GS−A_4865	Versionierte Liste zulässiger Firmware-Versionen	**FDP_ACF.1/AK.Update**
GS−A_4866	Integritäts- und Authentizitätsschutz der Firmware-Versionsinformationen	**FDP_ACF.1/AK.Update**
GS−A_4867	Übernahme Firmware-Gruppe	**FDP_ACF.1/AK.Update**
GS−A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	Die Nummerierung wird in der Umgebung (den Hersteller) sichergestellt.
GS−A_4869	Firmware-Gruppe mindestens eine Firmware-Version	Die Nummerierung wird in der Umgebung (den Hersteller) sichergestellt.
GS−A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe	**FDP_ACF.1/AK.Update**

GS−A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version	**FDP_ACF.1/AK.Update**
GS−A_4872	Kein Downgrade der Firmware-Gruppe	**FDP_ACF.1/AK.Update**
GS−A_4873	Speicherung der Firmware-Gruppe	**FDP_ACC.1/AK.Update** Signatur des Firmware Pakets ist integraler Teil des Firmware Pakets
GS−A_4874	Firmware-Gruppen-Updates nur über herstellereigenen Update-Mechanismus	**FDP_ACF.1/AK.Update**
GS−A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	Ist eine Anforderung für die Guidance und nicht das ST.
A_17124	TLS-Verbindungen (ECC-Migration)	**FCS_CKM.1/NK.TLS, FCS_COP.1/NK.TLS.Auth,** Anwendungshinweis 116:
A_17125	IKE-Schlüsselaushandlung für IPsec (ECC-Migration)	**FCS_COP.1/NK.Auth** und **FCS_CKM.1/NK** (Anwendungshinweis 110:)
A_17126	IPsec-Kontext -- Verschlüsselte Kommunikation (ECC-Migration)	**FCS_COP.1/NK.ESP**
A_21185	Prüfung der detached Signatur der TSL bei Download aus dem Internet	**FPT_TDC.1.2/AK,**
TIP1−A_4693−02	TUC_KON_032 „TSL aktualisieren”	**FPT_TDC.1.2/AK**
TIP1−A_4736−02	Kommunikation mit dem Internet (via IAG)	**FDP_IFF.1/NK.PF**
A_19052	Vorgaben für Dokumentformate und Nachrichten	Siehe „Gültiges XML-Schema“ Kapitel 9.3
A_19971	SGD und SGD-Client, Hashfunktion für Signaturerstellung und -prüfung	**FCS_COP.1/SGD.Auth** beschränkt sich auf SHA-256.
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	**FCS_COP.1/NK.TLS.Auth** zeigt die verwendeten TLS Algorithmen

A_21697	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	Siehe Anwendungshinweis 119:
A_21698	Importiertes Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Siehe **FMT_MTD.1/AK.Admin**
A_21699	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	Siehe Anwendungshinweis 194:
A_21701	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen exportieren	**FDP_ETC.2/NK.TLS** regelt den Export
A_21702	Intern generierte Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Siehe Anwendungshinweis 194:
A_21759	Aufgefrischte ID.AK.AUT für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Siehe Anwendungshinweis 194:
A_21760	ID.AK.AUT auf gSMC-K für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Siehe **FMT_MTD.1/AK.Admin**
A_22494	SGD-Client, HTTP-Variable SGD-Userpseudonym	FTP_ITC.1/SGD beschreibt den Kanal und Anmerkung 16 gibt genauere Informationen.

Tabelle 37: ST-Erweiterung für PTV5 (Weitere Anteile)

8.2. Erweiterungen für unterstützte Fachmodule

Der secunet konnektor 2.0.0 unterstützt die Fachmodule ePA (nach [49]), NFDM (nach [44]) und AMTS (nach [45]).

Entsprechend der Technischen Richtlinien TR-03154 ([24]) und TR-03155 ([25]), Kapitel 3.3.2 und TR-03157, Kapitel 3.2.2, gelten Anforderungen an den Konnektor die im Rahmen der CC Evaluierung betrachtet werden müssen. Diese werden im Folgenden zusammengefasst.

Der Anwendungskonnektor stellt den Fachmodulen ePA, NFDM und AMTS bestimmte Funktionen der Basisdienste zur Verfügung, die von den Fachmodulen über entsprechende Schnittstellen zum Konnektor aufgerufen werden können. In Tabelle 38 werden die nach TR-03157, TR-03154 und TR-03155 sicherheitsrelevanten Funktionen der Basisdienste anhand der in [27] definierten Technical Use Cases (TUC) aufgelisteten und die jeweilige dem Fachmodul angebotene Schnittstelle angegeben.

Dienst nach [27]	**TUC nach [27]**	**Konnektor-Schnittstelle zum Fachmodul**	**Fach-module**
Zugriffsberechtigungsdienst	TUC_KON_000 „Prüfe Zugriffsberechtigung“	[Fachmodul-API]	NFDM, AMTS, ePA
Dokumentenvalidierungsdienst	TUC_KON_080 „Dokument validieren“ (indirekt)	[Fachmodul-API]	NFDM
Für Schlüsselerzeugung	TUC_KON_072 „Daten symmetrisch verschlüsseln“	[Fachmodul-API]	ePA
Kartendienst	TUC_KON_005 „Card-to-Card authentisieren“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	[Fachmodul-API]	NFDM, AMTS
Kartendienst	TUC_KON_012 „PIN verifizieren“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_018 „eGK-Sperrung prüfen“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_022 „Liefere PIN-Status“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_023 „Karte reservieren“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_026 „Liefere CardSession“	[Fachmodul-API]	NFDM, AMTS, ePA
Kartendienst	TUC_KON_036 „Liefere Fachliche Rolle“	[Fachmodul-API]	NFDM, AMTS
Kartendienst	TUC_KON_041 „Einbringen der Endpunktinformationen während der Bootup-Phase“	[Fachmodul-API]	NFDM, AMTS
Kartendienst	TUC_KON_202 „Lese Datei“	[Fachmodul-API]	NFDM, AMTS

Kartendienst	TUC_KON_203 „Schreibe Datei“	[Fachmodul-API]	NFDM, AMTS
Kartendienst	TUC_KON_204 „Lösche Datei Inhalt“	[Fachmodul-API]	NFDM, AMTS
Kartenterminaldienst	TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	[Fachmodul-API]	NFDM, AMTS
Namensdienst	TUC_KON_361 „DNS-Namen auflösen“	[Fachmodul-API]	ePA
Namensdienst	TUC_KON_362 „Liste der Dienste abrufen“	[Fachmodul-API]	ePA
Namensdienst	TUC_KON_363 „Dienstdetails abrufen“	[Fachmodul-API]	ePA
Signaturdienst	TUC_KON_151 „QES Dokumentensignatur prüfen“	[Fachmodul-API]	NFDM
Signaturdienst	TUC_KON_160 „Dokumente nonQES signieren“	[Fachmodul-API]	ePA
Signaturdienst	TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“	[Fachmodul-API]	NFDM
Systeminformationsdienst	TUC_KON_254 „Liefere Ressourcendetails“	[Fachmodul-API]	NFDM, AMTS, ePA
TLS-Dienst	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	[Fachmodul-API]	ePA
TLS-Dienst	TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	[Fachmodul-API]	ePA
Protokollierungsdienst	TUC_KON_271 „Schreibe Protokolleintrag“	[Fachmodul-API]	NFDM, AMTS, ePA
Verschlüsselungdienst	TUC_KON_075 „Symmetrisch verschlüsseln”	[Fachmodul-API]	ePA
Verschlüsselungdienst	TUC_KON_076 „Symmetrisch entschlüsseln”	[Fachmodul-API]	ePA
Zeitdienst	TUC_KON_351 „Liefere Systemzeit“	[Fachmodul-API]	NFDM, AMTS, ePA
Zertifikatsdienst	TUC_KON_034 „Zertifikatsinformationen extrahieren“	[Fachmodul-API]	NFDM, ePA
Zertifikatsdienst	TUC_KON_037 „Zertifikat prüfen“	[Fachmodul-API]	ePA
Für leichtgewichtige Sicherungsschicht	Interne Schnittstellen zum Client für leichtgewichtige Sicherungsschicht auf Anwendungsebene	[Fachmodul-API]	ePA
Client für beidseitig authentisierten Ende-zu-Ende-verschlüsselten Kanal mit SGD-HSDM	Interne Schnittstellen für die ECIES-basierte Kommunikation zwischen Konnektor Basisfunktionalität und zwei SGD-HSMs gemäß	[Fachmodul-API]	ePA

Tabelle 38: Sicherheitsrelevante Schnittstellen zu den Fachmodulen

Die Prüfung der korrekten Nutzung der Schnittstellen durch die Fachmodule ist Gegenstand der TR-Zertifizierung nach den Technischen Richtlinien TR-03157, TR-03154 und TR-03155. Im

Rahmen der CC-Zertifizierung wird die korrekte und sichere Umsetzung der Funktionalität durch den Konnektor geprüft, siehe dazu auch 6.4.2, Verfeinerungen hinsichtlich der Fachmodule NFDM, AMTS.

Darüber hinaus werden in den Technischen Richtlinien zur Prüfung der Fachmodule weitere Sicherheitsanforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung betrachtet werden müssen. Diese werden in der folgenden Tabelle diskutiert:

Anforderungen aus TR	**Umsetzung durch den Konnektor**
(Nur NFDM) Signaturdienst – QES-Prüfung von XML-detached Signaturen (nach vorheriger Prüfung gemäß gematik Signaturrichtlinie für gematik-vorgegebenem XML Schema)	Die QES-Prüfung von XML-detached Signaturen ist Sicherheitsfunktionalität des Konnektors und Gegenstand der Zertifizierung. Das Fachmodul NFDM stellt dem Konnektor eine Signaturrichtlinie mit dem gematik-vorgegebenem XML Schema zur Verfügung. Im SFR FPT_TDC.1/AK wurden die Interpretation der Signaturrichtlinien des NFDM Fachmoduls entsprechend berücksichtigt und ist damit Sicherheitsfunktionalität des EVGs. Entsprechend O.AK.Sig.SignQES wird die Wohlgeformtheit der zu signierenden Dokumente gegen die entsprechende Format-Spezifikation geprüft. Das beinhaltet für Fachmodule die Prüfung gegen das in der Signaturrichtline festgelegte XML Schema.
Gültigkeitsprüfung der eGK	Die Gültigkeitsprüfung der eGK wird durch das Sicherheitsziel O.AK.Chipkartendienst umgesetzt und ist damit Sicherheitsfunktionalität des EVGs: FPT_TEE.1/**AK** fordert bei Stecken einer Chipkarte, die vorgibt, ein HBA, eine gSMC-KT, eine SMC-B oder eine eGK zu sein, zu prüfen, ob sie tatsächlich eine solche Chipkarte ist. Die dafür präsentierten CV-Zertifikate werden gemäß FPT_TDC.1/**AK** auf Gültigkeit für HBA, SMC (gSMC-KT oder SMC-B) und eGK geprüft.
Funktionalität des Konnektors zur Transportsicherung zwischen Konnektor und Clientsystem	Die Transportsicherung zwischen Konnektor und Clientsystem wird durch die Sicherheitsfunktionen NK.TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen und AK.TLS-Kanäle umgesetzt und ist damit Sicherheitsfunktionalität des EVGs

Auslesbare, eindeutige Version des Konnektors sowie des Fachmoduls NFDM und AMTS.	Die Version der Fachmodule lässt sich über die Management-Schnittstelle des Konnektors auslesen. Im Benutzerhandbuch findet sich die entsprechende Beschreibung.
(Nur ePA) Rollenprüfung im TLS-Dienst	Das Fachmodul ePA definiert beim Verbindungsaufbau für das TLS-Zertifikat der Gegenstelle eine zulässige Rolle. Werden die Anforderungen des Fachmoduls an das Zertifikat der Gegenstelle nicht erfüllt, MUSS der Konnektor die Verbindung abbrechen. Die Rollenprüfung von Zertifikaten wird mit TUC_KON_036 umgesetzt.
(Nur ePA) Rollenprüfung in der Basisfunktionalität ‚leichtgewichtige Sicherungsschicht zur VAU'	Weist das Zertifikat der VAU nicht die Rolle *oid_epa_vau* (*nach [50]*) auf, MUSS der Konnektor die Verbindung abbrechen. Dies ist umgesetzt in FTP_ITC.1/VAU.

Tabelle 39: Weitere Anforderungen an den Konnektor

8.3. Informationen zur Signaturdirektive

Der Konnektor setzt im Signaturdienst (siehe Kapitel AK.Signaturdienst) verschiedene Signaturtypen und Signaturvarianten um und erlaubt es, optional sogenannte Signaturrichtlinien in Operationsaufruf anzugeben, die sicherstellen, dass entsprechend erzeugte Dokumenten-Siganturen einem vorgegebenen Schema folgen. Dabei wird der Begriff „Signaturrichtlinie“ in Rahmen der Konnektorevaluierung unterschiedlich verwendet:

a) Signaturrichtlinie als im Operationsaufruf angegebene Richtlinie für genau diese Dokumenten-Signatur. Das entspricht der Auffassung einer Signaturrichtlinie nach [gemSpec_Kon]
b) Signaturrichtlinie als allgemeine funktionale Einschränkung der Konnektor-Schnittstelle.

Bei der NFDM-Signaturrichtlinie [46] handelt es sich zum Beispiel um eine Signaturrichtlinie nach erster Definition. Zur Abgrenzung der Begrifflichkeiten wird bei einer Signaturrichtlinie nach zweiter Definition von einer Signaturdirektive gesprochen.

Im Dokument [113] wird die Signaturdirektive des secunet konnektor 2.0.0 beschrieben. Die Härtung der entsprechenden Schnittstellen (z.B. Härtung des XML-Parsers) wird im Dokument [114] beschrieben.

8.4. Informationen zur Verschlüsselungsdirektive

Der Konnektor bietet durch den Verschlüsselungsdienst den Clientsystemen die Möglichkeit Dokumente hybrid zu ver- und entschlüsseln. Analog zur „Signaturrichtlinie“ des Signaturdienstes wird der Begriff „Verschlüsselungsrichtlinie“ in Rahmen der Konnektorevaluierung unterschiedlich verwendet:

a) Verschlüsselungsrichtlinie als im Operationsaufruf angegebene Richtlinie für genau diese Dokumenten-Verschlüsselung.
b) Verschlüsselungsrichtlinie als allgemeine funktionale Einschränkung der Konnektor-Schnittstelle.

Eine Verschlüsselungsrichtlinie nach a) ist in [gemSpec_Kon] nicht spezifiziert und wird von Konnektor nicht unterstützt. Es können keine solche Verschlüsselungsrichtlinien im Operationsaufruf angegeben werden. Zur Abgrenzung der Begrifflichkeiten wird bei einer Verschlüsselungsrichtlinie nach Definition b) von einer Verschlüsselungsdirektive gesprochen.

Im Dokument [115] wird die Verschlüsselungsdirektive des secunet konnektor 2.0.0 beschrieben. Die Härtung der entsprechenden Schnittstellen (z.B. Härtung des XML-Parsers) wird im Dokument [114] beschrieben.

9. Anhang

9.1. Auszüge aus der Konnektorspezifikation [27] zum Zugriffsberechtigungsdienst

Siehe die folgenden Tabellen in Kapitel 7.1 des Protection Profiles [16]:

- Tabelle 29: TAB_KON_507 Informationsmodell Entitäten aus [27]
- Tabelle 30: TAB_KON_508 Informationsmodell Attribute aus [27]
- Tabelle 31: TAB_KON_509 Informationsmodell Entitätenbeziehungen aus [27]
- Tabelle 32: TAB_KON_510 Informationsmodell Constraints aus [27]
- Tabelle 33: TAB_KON_511 – TUC_KON_000 „Prüfe Zugriffsberechtigung“ aus [27]
- Tabelle 34: TAB_KON_512 Zugriffsregeln Beschreibung
- Tabelle 35: TAB_KON_513 Zugriffsregeln Regelzuordnung aus [27]
- Tabelle 36: TAB_KON_514 Zugriffsregeln Definition aus [27]

9.2. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AK	Anwendungskonnektor
ECIES	Elliptic Curve Integrated Encryption Scheme
EVG	Evaluierungsgegenstand
AP	Arbeitsplatz (entspricht dem Clientsystem)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BnetzA-VL	Vertrauensliste der Bundesnetzagentur
CHA	Card holder autorization, Rechte, die ein Zertifikatsinhaber besitzt
CHAT	Card Holder Authorization Table, Liste der Zugriffsrechte (Flaglist) des Karteninhabers
CA	Certification Authority, Zertifizierungsinstanz
CadES	CMS Advanced Electronic Signature: Standard (RFC 5126) zur Definition von Profilen für CMS signierte Daten
CMS	im Kontext von Fachanwendungen: Card Management System, Kartenmanagementsystem im Kontext digitaler Signaturen: Cryptographic Message Syntax
CORS	Cross-origin Resource Sharing
CRL	Certificate Revocation List
CVC	Card verifiable certificate, kartenverifizierbares Zertifikat
DTBS	data 400ob e signed (zu signierende Daten)
EAL	Evaluation Assurance Level (vordefinierte Vertrauenswürdigkeitsstufe in den CC)
eGK, eHC	elektronische Gesundheitskarte (Englisch: eHC, electronic Health Card)

eIDAS	eIDAS-Verordnung (electronic identification and trust services for electronic transactions)
EVG	Evaluierungsgegenstand (Prüfgegenstand der Evaluierung), engl: target of evaluation (TOE)
gematik	gematik GmbH, siehe www.gematik.de
HBA	Heilberufsausweis, Englisch: Health Professional Card (HPC)
HBAx	Bezeichnung für Chipkarten des Typs HBA, HBA-qSig und ZOD-2.0
HKDF	HMAC-based Key Derivation Function
HSM	Hardware Security Module
HSM-B	Eine HSM-Variante einer Institutionskarte Typ B (Secure Module Card). Das SM-B wird in dieser Fassung als virtuelle Karte verstanden, welches in einem virtuellen Kartenterminal steckt.
HW	Hardware
IAG	Internetzugangspunkt des Leistungserbringers
JSON	JavaScript Object Notation
KT	Kartenterminal, Englisch: Cardterminal (CT)
KV	Krankenversicherung
KVK	Krankenversichertenkarte
LAN	local area network (lokales Netzwerk)
LE	Leistungserbringer
LE-LAN	lokales Netz der Leistungserbringer
MAC	Message Authentication Code
NK	Netzkonnektor
OCSP	Online Certificate Status Protocol, siehe RFC 2560

PAdES	PDF Advanced Electronic Signature: ETSI Standard zur Signatur von PDF Dokumenten
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PP	Protection Profile (Schutzprofil)
PUK	PIN unblock code zum Rücksetzen des Fehlbedienungszählers des Heilberufsausweises.
PVS	Praxisverwaltungssystem
RAD	reference authorisation data (Authentisierungsreferenzdaten)
SE	Security environment
SAK	Bezeichnung einer Identität des Konnektors; steht für Signaturanwendungs-komponente, einem Begriff aus dem SigG. Um Missverständnissen vorzubeugen, wurde im Rahmen der Aktualisierung dieses PPs aufgrund der eIDAS Verordnung der Begriff SAK durch SCaVA ersetzt.
SCA	Signature Creation Application
SVA	Signature Validation Application
SCaVA	Signature Creation Application and Signature Validation Application
SCD	signature creation data (Signaturschlüssel)
SICCT	Secure Interoperable Chip Card Terminal
SigG	Deutsches Signaturgesetz
SigV	Deutsche Signaturverordnung
SIS	Sicherer Internet Service
SM	secure messaging (sicherer logischer Kanal)

SMC-B	Secure Module Card, Type B (Institutskarte): Schlüsselspeicher für den privaten Schlüssel, mit dessen Hilfe eine Einheit oder Organisation des Gesundheitswesens authentisiert werden kann
SM-B	Zusammenfassung der Chipkarten SMC-B und HSM-B
SM-K	Sicherheitsmodul für den Konnektor (kann gSMC-K beinhalten)
gSMC-K	Sicherheitsmodul für den Konnektor
gSMC-KT	Sicherheitsmodul für das eHealth-Kartenterminal
QES	qualifizierte elektronische Signatur
QSCD	Englisch: qualified signature-creation device, siehe QSEE
QSEE	qualifizierte elektronische Signaturerstellungseinheit
SVAD	Signatory Verification Authentication Data (Authentisierungsverifikations-daten des Signaturschlüsselinhabers)
SVD	signature verification data (Signaturprüfschlüssel)
SW	Software
TCL	Trusted Component List
TI	Telematikinfrastruktur
TLS	Transport layer security, standardisiertes sicheres Kommunikationsprotokoll
TSL	Trust-service Status List
TSP	Trusted Service Provider
VDA	Vertrauensdiensteanbieter
VSD	Versichertenstammdaten
VSDM	Versichertenstammdatenmanagement, siehe auch Fachmodul
VSDD	Versichertenstammdatendienst, siehe auch Fachdienst
XAdES	XML Advanced Electronic Signature: ETSI Standard zur Signatur von XML Dokumenten

XAdES-X	XAdES extended: ein Profil von XAdES
xTV	Veraltete Bezeichnung eines Teils einer SAK gemäß SigG/SigV. Extended Trusted Viewer (erweiterte sichere Anzeige) als Teil des Konnektors, ausgelagert auf den Arbeitsplatz des Benutzers. Diese Funktionalität kann nun von einer Clientsoftware umgesetzt werden und gehört nicht zum EVG.

Tabelle 40: Abkürzungsverzeichnis

9.3. Glossar

Begriff	Definition
Ablauflogik	Der Begriff Ablauflogik bezeichnet die Möglichkeit, erlaubte Reihenfolgen von Basisdiensten und Fachdiensten vorzugeben. Welche Abläufe dies im Einzelnen sind, hängt von den konkreten fachlichen Anwendungsfällen ab. Die Ablauflogik kann außerhalb der TSF liegen, die Ablaufkontrolle ist Teil der TSF. Häufig wird der Begriff Ablauflogik auch synonym zum Begriff Fachlogik verwendet.
Anwendungs-konnektor	Der Teil des Konnektors [27], der dem Clientsystem die Schnittstellen zu den Fachdienstmodulen (VSDD, AMTS etc.) und Basisdienste (Sicherheitsdienste, Chipkartendienste, Kartenterminaldienste, Hilfsdienste) zur Verfügung stellt und die dafür notwendigen Managementdienste implementiert.
Authentisierungs-referenzdaten	Daten, die zur Prüfung der Authentisierungsdaten benutzt werden. Die Integrität dieser Authentisierungsreferenzdaten ist zu schützen. Englisch: authentication reference data, abgekürzt RAD.
Authentisierungs-verifikationsdaten	Daten, die vom Benutzer zum Nachweis seiner Identität gegenüber dem Kartenterminal präsentiert werden, z.B. eine PIN oder biometrische Merkmalsdaten. Englisch: authentication verification data, abgekürzt SVAD.
Autorisierter Benutzer des Clientsystems	Ein Benutzer des Clientsystems ist dann für die Auslösung des Signaturprozesses autorisiert, wenn der Benutzer durch den EVG identifiziert wurde, sich für den Vorgang, der durch die am eHealth-Kartenterminal angezeigte Jobnummer identifiziert wurde, gegenüber dem zugeordneten Heilberufsausweis erfolgreich mit der PIN.QES authentisiert hat (vergl. [21]).
Autorisierter Signaturstapel	Derjenige Teil eines Stapels zu signierender Daten (s.u.), der nach erfolgreicher Authentisierung des Signaturschlüsselinhabers mit der

	Signatur-PIN gegenüber der Signaturchipkarte durch den Signaturdienst an die Signaturkarte zum Signieren gesendet wird. Umfasst der Stapel zu signierender Daten mehr Daten als durch die Zugriffsbedingung der Signaturkarte nach eine Authentisierung mit der Signatur-PIN zulässig sind, ist die Authentisierung mit der Signtaur-PIN zu wiederholen oder Prozess der Signaturerstellung abzubrechen (s.a. Anwendungshinweis 191:).
Bestandsnetz	Bereits vor Einführung der Telematikinfrastruktur bestehende Netze deren Anwednungen durch Leistungserbringer genutzt werden und über die Telematikinfrastruktur zugänglich sind.
Kartenhandle (BKH)	Handle zur Identifizierung einer Chipkarte, die in einem eHealth-Kartenterminal steckt. Mit diesem BKH sind folgende Informationen verknüpft (s. [27], Kap. 4.1.1.1): (i) Chipkartentyp KVK, bzw. HBA, SMC oder eGK, (ii) ICCSN, (iii) Identität des Kartenterminals, in dem die Chipkarte gesteckt ist und (iv) Zeitpunkt, zu dem die Chipkarte erkannt wurde.
Card-to-Card-Authentisierung	Card-to-Card-Authentisierung umfasst (s. [27], Kap. 4.1.5.4.7): (1) einseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, (2) einseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, (3) gegenseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, (4) gegenseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, (5) gegenseitige asymmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals, (6) gegenseitige symmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals. Die externe Authentisierung mit Ausnahme von (5) verändert den Authentisierungsstatus der prüfenden Chipkarte.
Chipkarte	In diesem Schutzprofil: der Heilberufsausweis (HBA), SMC-Typ B, eGK und KVK.
CRL Download Server	Ein von der PKI der TI bereitgestellter Downloadpunkt im Internet, von dem der Konnektor die aktuelle CRL erhalten kann.
Digitale Signaturen	Asymmetrischer kryptographischer Mechanismus bei dem für Daten („Nachricht“) ein Datum („Signatur“) mit Hilfe eines geheimen

	Signaturschlüssels („Signaturerstellungsdaten“) berechnet und der Nachricht zugeordnet werden, und diese Zuordnung bei Kenntnis der Nachricht und der Signatur mit dem zum Signaturschlüssel zugehörigen öffentlichen Signaturprüfschlüssel geprüft werden kann.
eIDAS-Verordnung	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [12].
eingeschränkter Text	Text, der keine unerlaubten Zeichenketten enthält, die den Benutzer des Kartenterminals zur Eingabe einer PIN oder PUK im ungeschützten Mode verleiten könnte.
eHealth-Kartenterminal	Kartenterminal gemäß Spezifikation [38], evaluiert gemäß [22] und als Signaturprodukt zugelassen.
Einfachsignatur	Die qualifizierte Signaturerstellungseinheit (QSEE) erlaubt nach einmaliger erfolgreicher Authentisierung des Signaturschlüssel-Inhabers die Erzeugung höchstens 1 Signatur.
Elektronische Signaturen	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet, vergl. eIDAS [12] Artikel 3, Punkt 10.
Entfernte PIN-Eingabe	Prozess der eine Eingabe der PIN (oder PUK) an einem eHealth-Kartenterminal (PIN-Terminal) und geschützte Übertragung durch eine gSMC-KT (PIN-Sender) an eine Chipkarte (PIN-Empfänger) in einem anderen Chipkarten-Terminal unter Steuerung der AK (s. [21], Kap. 2.1.2, und [27], Kap. 4.1.5.5.1). Die entfernte PIN-Eingabe muss den sicheren Eingabe-Modus der eHealth-Kartenterminals und die Jobnummer nutzen und die PIN verschlüsselt an den PIN-Empfänger übergeben. Die Prozeduren der entfernten PIN- oder PUK-Eingabe können auch für eine lokale PIN- oder PUK-Eingabe genutzt werden (d.h. ein einziges eHealth-Kartenterminal dient der PIN-Eingabe und enthält gesteckten PIN-Sender und PIN-Empfänger).
Fachanwendung	Anwendung die durch Fachmodul und Fachdienst realisiert wird. Gelegentlich wird aber auch allgemeiner eine fachliche Anwendung darunter verstanden wie in § 291 a SGB V [14], definiert (Abs. (2): Pflichtanwendungen, Abs. (3): freiwillige Anwendungen): • Übermittlung ärztlicher Verordnungen (Verordnungsdaten-management, VODM), • Berechtigungsnachweis zur Inanspruchnahme von Leistungen (Versichertenstammdatenmanagement, VSDM),

	• Notfallversorgung (Notfalldatenmanagement, NFDM), • Arztbrief • Arzneimitteltherapiesicherheit • elektronische Patientenakte • Versichertendaten • in Anspruch genommene Leistungen und deren vorläufige Kosten Siehe auch Fachdienst und Basisanwendung.
Fachdienst	der Teil einer fachlichen Anwendung (siehe auch Fachliche Anwendungsfälle), der entfernt abläuft – in Abgrenzung zu Fachmodul (im Konnektor) und Fachanwendung (auf dem Clientsystem). Für Online-Rollout Stufe 1 gibt es nur den Fachdienst VSDM (Versichertenstammdatenmanagement).
Fachliche Anwendungsfälle	einzelne Anwendungsfälle (Use Cases) innerhalb einer Fachanwendung (siehe auch Fachanwendung). In Dokumenten zur Facharchitektur (von Fachanwendungen) werden solche fachlichen Anwendungsfälle auch als fachliche Use Cases bezeichnet. Die fachlichen Use Cases werden durch technische Use Cases umgesetzt. Technische Use Cases werden auch als Abläufe bezeichnet.
Fachmodul	der Teil einer fachlichen Anwendung (siehe auch Fachliche Anwendungsfälle), der auf dem Konnektor abläuft – in Abgrenzung zu Fachanwendung (auf dem Clientsystem) und Fachdienst. Siehe auch Ablauflogik
Fortgeschrittene elektronische Signaturen	elektronische Signatur, die die folgenden Anforderungen erfüllt: a) Sie ist eindeutig dem Unterzeichner zugeordnet. b) Sie ermöglicht die Identifizierung des Unterzeichners. c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann. vergl. eIDAS [12] Artikel 3, Punkt 11 und Artikel 26
Gültige Verschlüsselungs-richtlinie	Eine zulässige Verschlüsselungsrichtlinie ist gültig, wenn sie durch den autorisierten Benutzer für die zu verschlüsselnden oder zu entschlüsselnde Daten bestätigt oder durch die Nutzung der Fachanwendung bzw. des Anwendungsfalls festgelegt wurde.

Gültiges qualifiziertes Signaturzertifikat	Die Gültigkeit eines qualifizierten Zertifikates erfordert die Erfüllung der Aspekte im Zertifikatsverzeichnis vorhanden, zeitliche Gültigkeit und Revocation-Status: Gültige Zertifikate müssen im Zertifikatsverzeichnis des ausstellenden qualifizierter Vertrauens-diensteanbieters vorhanden sein. Der Vertrauensdiensteanbieter ist nach eIDAS [12] Artikel 24, Absatz 4 verpflichtet, Informationen über den Gültigkeits- oder Widerrufsstatus der von ihnen ausgestellten qualifizierten Zertifikate zumindest auf Zertifikatsbasis jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch auf zuverlässige, kostenlose und effiziente Weise bereitzustellen. Die zeitliche Gültigkeit liegt dann vor, wenn der zu dem der Prüfung zugrundeliegende Referenzzeitpunkt innerhalb des im Zertifikat angegebenen Gültigkeitszeitraum liegt. Der Revocation Status ist gültig, wenn das Zertifikat zu dem der Prüfung zugrundeliegende Referenzzeitpunkt nicht gesperrt ist.
Gültiges Zertifikat	Die Gültigkeit eines Zertifikats kann unter Verwendung einer Zertifikatspolicy und im Fall eines qualifizierten Zertifikats einer OCSP-Anfrage festgestellt werden.
Gültiges XML-Schema	Ein im EVG fest kodiertes oder mit gültiger Signatur importiertes XML-Schema, siehe auch A_19052.
Gültiges Verschlüsselungs-zertifikat der TI	Ein Verschlüsselungszertifikat ist gültig, wenn (i) seine Integrität durch eine Zertifikatskette bis zu einem authentisch bekannten öffentlichem Schlüssel erfolgreich geprüft wurde und (ii) das Verschlüsselungszertifikat nicht gesperrt ist. Für ein Verschlüsselungszertifikat eines Versicherten, das von einer aktuell gesteckten eGK gelesen wird, kann explizit angenommen werden, dass es nicht gesperrt ist. Eine Sperrung anderer Verschlüsselungszertifikate ist mittels OCSP-Abfrage zu prüfen.
hash&URL server	Der hash&URL-Server ist ein http-Server, der die zur gegenseitigen Authentifizierung von Konnektoren und VPN-Konzentratoren genutzten Zertifikate gemäß [RFC7296] zum Download bereitstellt.
Heilberufsausweis (HBA)	Chipkarte gemäß Spezifikation [31] und [35], dessen Betriebssystem nach PP COS G2 [15] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.
HBA-Vorläuferkarten (HBA-VK)	Adressiert die HBA-Vorläuferkarten HBA-qSig und ZOD_2.0. Wird dieser Referenzbezeichner verwendet, gelten die zugehörigen Aussagen und Festlegungen für beide Kartentypen. (vergl. [27], TAB_KON_500 Wertetabelle Kartentypen).

HBAx	Adressiert sowohl den HBA, als auch die HBA-Vorläuferkarten (HBA-VK). Wird dieser Referenzbezeichner verwendet, gelten die zugehörigen Aussagen und Festlegungen für alle drei Kartentypen.
ICCSN	Seriennummer des Chipkartenchips (engl. ICC Serial Number)
Intermediär	Vermittler zwischen zwei Systemen, wobei beide Systeme jeweils dem Intermediär vertrauen, nicht jedoch zwangsweise einander.
Konnektor	dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Leistungserbringer an die Telematikinfrastruktur und Steuerung der eHealth-Kartenterminals im LAN des Leistungserbringers gemäß [27].
Krankenversicherten-karte (KVK)	Chipkarte mit eingeschränkter Funktionalität, die die Identität des Versicherten speichert. Die KVK besitzt kein EF.ATR, EF.GDO und EF.DIR und kann keine PIN-Authentisierung, Card-to-Card-Authentisierung und keine Zugriffskontrolle durchführen.
Leistungserbringer	Verantwortlicher für die Einsatzumgebung der dezentralen Komponenten Konnektor, eHealth-Kartenterminal und SMC Typ B sowie der Clientsysteme und des lokalen Netzes.
lokale PIN-Eingabe	Die PIN-Eingabe erfolgt an dem Chipkartenterminal, in welchem sich die Chipkarte befindet, die die PIN prüfen soll. Die lokale PIN-Eingabe nutzt den sicheren Eingabe-Modus der eHealth-Kartenterminals und darf die PIN sowohl unverschlüsselt als auch mit den Prozeduren der entfernten PIN-Eingabe verschlüsselt an den PIN-Empfänger übergeben.
Managementschnitt-stelle	(herstellerspezifische) äußere logische Schnittstelle für alle Managementfunktionen einschließlich Administratorfunktionen.
Ordnungsgemäße qualifizierte elektronische Signaturen eines Signaturstapel	Ordnungsgemäße qualifizierte elektronische Signaturen sind solche fortgeschrittene elektronische Signaturen, die zu den Daten des Signaturstapels mit dem Signaturschlüssel des Heilberufsausweises des autorisierten Benutzers des Clientsystems erzeugt wurden und zu dessen Signaturprüfschlüssel zum für die Signatur festgelegten Zeitpunkt ein gültiges qualifiziertes Zertifikat existiert.
PIN-Empfänger	Chipkarte, die eine verschlüsselte PIN oder PUK verschlüsselt für die PIN-Prüfung oder den PIN-Wechsel oder das Entblockieren einer PIN empfängt. Ein PIN-Empfänger ist ein HBA oder eine SMC-B (oder ein RFID-Token für die Komfortsignatur, wenn der EVG Komfortsignatur mit derartigen Token unterstützt).

PIN-Sender	Chipkarte, die eine PIN oder PUK unverschlüsselt empfängt und verschlüsselt für die Übertragung an den PIN-Empfänger ausgibt. Ein PIN-Sender ist eine gSMC-KT.
Clientsystem	Komponente mit einem Benutzerinterface für fachliche Funktionalität. Die Clientsysteme der Leistungserbringer umfassen die Praxisverwaltungssysteme, für Ärzte und Zahnärzte, die Krankenhausinformationssysteme der Krankenhäuser und die Apothekenverwaltungssysteme der Apotheker und stellen die Anwendungsprogramme für die Leistungserbringer und Versicherten zur Verfügung. Sie sind über das LAN des Leistungserbringers mit dem Konnektor verbunden.
qualifizierte elektronische Signaturen	Fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht, vgl. eIDAS [12] Artikel 3 Punkt 12. Abgekürzt QES.
qualifizierter elektronischer Zeitstempel	Ein elektronischer Zeitstempel, der Datum und Zeit so mit Daten verknüpft, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist, vgl. eIDAS [12] Artikel 3 Punkt 34 und Artikel 42.
qualifiziertes Zertifikat	Ein: „Qualifiziertes Zertifikat für elektronische Signaturen“ ist ein von einem qualifizierter Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen aus eIDAS [12] Anhang I erfüllt.
qualifizierter Vertrauensdienste-anbieter	„Qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde vgl. eIDAS [12] Artikel 3 Punkt 20.
Registration server of the VPN network provider	Der Registrierungsserver ist ein http-Server, welcher Anfragen des Konnektors zur Registrierung des Konnektors durch den berechtigten Teilnehmer beim Anbieter entgegennimmt und bearbeitet.
remote management server	Management-Gegenstelle für das Remote-Management des Konnektors (sofern dieses angeboten wird).
Security environment SE#1 und SE#2	Security environment sind spezielle Sicherheitszustände des HBA, die Zugriffsregeln für die Erzeugung digitaler Signaturen für qualifizierte elektronische Signaturen setzen (s. [35], Kap. 9).
qualifizierte elektronische Signaturerstellungs-einheit	Konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird und die Anforderungen aus eIDAS [12] Anhang II erfüllt; Abkürzung: QSEE. Englisch:QSCD.

Sicherer PIN-Modus	Tastatureingabemodus des eHealth-Kartenterminals gemäß [38], in dem das eHealth-Kartenterminal durch ein SICCT-Kommando [42] angewiesen wird, die Tastatureingabedaten in einem angegebenen Chipkartenkommando an eine Chipkarte in einem angegebenen Chipkartensteckplatz zu senden und die Antwort der Chipkarte zurückzugeben. Der sichere PIN-Modus ist dem Benutzer anzuzeigen und muss die Vertraulichkeit der Tastatureingabedaten schützen.
Signaturanwendungs-komponenten	Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate Englisch: SCA und SVA, hier als SCaVA abgekürzt.
Signaturattribute	Dieser Begriff wird hier verwendet, um die Arten der Signaturen „einfache Dokumentensignatur“, „Parallelsignatur“ und „Gegensignatur“ zu unterscheiden. Sicherheitsattribute sind Bestandteil der Signaturrichtlinie.
Signaturchipkarte	Chipkarte mit privaten Schlüsseln zur Erstellung digitaler Signaturen einer elektronischen Signatur. Dies sind gegenwärtig der HBA mit dem privaten Schlüssel PrK.HP.QES, die SMC Typ B mit dem privaten Schlüssel PrK.HI.OSIG und die eGK mit dem privaten Schlüssel PrK.CH.QES.
Signaturrichtlinie	Die Signaturrichtlinie (Profilierung der Signaturformate) identifiziert - den Typ der Signatur als nicht-qualifizierte oder qualifizierte elektronische Signatur, und kann weitere Informationen umfassen (s. [27], Anhang B) wie z.B. - Anforderungen an Zertifikatsreferenzen - Anforderungen an die Position der Signatur im Dokument - Signaturattribute: Anforderungen bei u.a. Parallelsignatur, dokumentexkludierende Gegensignatur und dokumentinkludierende Gegensignatur für die i.A. spezifizierten unterschiedlichen Signaturformate XAdES, CadES und PAdES. - Bitstrings bei PKCS#7 - U.a.
Signaturprüfschlüssel	elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden, Englisch: signature-verification data, abgekürzt SVD.

Signaturschlüssel	einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden, Englisch: signature-creation data, abgekürzt SCD.
Signaturschlüssel-Inhaber	natürliche Personen, die Signaturschlüssel besitzen; bei qualifizierten elektronischen Signaturen müssen ihnen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sein.
Signaturzertifikate	elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.
Signierte Daten	Daten auf die sich eine digitale Signatur einer elektronischen Signatur bezieht.
Signature Creation Application	Begriff aus den ETSI Standards. Bezeichnet eine Komponente, die Signaturen (auch) gemäß eIDAS erzeugt. Abgekürzt SCA.
Signature Validation Application	Begriff aus den ETSI Standards. Bezeichnet eine Komponente, die Signaturen (auch) gemäß eIDAS validiert/verifiziert. Abgekürzt SVA.
SM-B	Oberbegriff von SMC-B und einem HSM mit Funktionen oder Teilfunktionen einer SMC-B.
SMC	Sicherheitsmodul-Karte. Sammelbegriff für gSMC-K, SMC-B und gSMC-KT.
SMC Typ B (SMC-B)	Chipkarte gemäß Spezifikation [31] und [36], dessen Betriebssystem nach PP COS G2 [15] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.
SMC Typ KT (gSMC-KT)	Sicherheitsmodul des Kartenterminals. Chipkarte gemäß Spezifikation [31] und [34], dessen Betriebssystem nach PP COS G2 [15] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.
gSMC-K	Sicherheitsmodul des Konnektors. Teil des EVG mit denjenigen Schlüsseln und diejenige Funktionalität, die für die Aufgaben des EVG wie die Authentisierung und Secure messaging mit der Identität „SAK“ gegenüber dem HBA benötigt werden. Chipkarte gemäß Spezifikation [31] und [33], die durch die gematik zugelassen wurden.
Stapel zu signierender Daten	Liste zu signierender Daten, die durch den Benutzer des Clientsystems ausgewählt wurden und über das Clientsystem an den EVG gesendet wurden.

Stapelsignatur	Erstellung einer begrenzten Anzahl Signaturen nach den zeitlich unmittelbar aufeinander folgenden Prozessen der Übergabe der zu signierenden Daten an den EVG über das Clientsystem und der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der QSEE.
stateful packet inspection, stateful inspection	dynamische Paketfiltertechnik, bei der (sofern es die Systemressourcen zulassen; im Fall eines denial-of-service-Angriffs müssen Datenpakete verworfen werden) jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird; der Verbindungsstatus eines Datenpakets wird in die Entscheidung einbezogen, ob ein Informationsfluss zulässig ist oder nicht
Statusmeldungen	Durch den EVG generierte Meldungen an Benutzer zu Fehlern bei der Erfüllung angeforderter Sicherheitsdienst (z. B. nicht gefundene oder ungültige Zertifikate vorgesehener Empfänger zu verschlüsselnder Daten).
Telematikinfrastruktur (TI)	Die Telematikinfrastruktur ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen und organisatorischen Anteilen. Die Telematikinfrastruktur vernetzt alle Akteure und Institutionen des Gesundheitswesens miteinander und ermöglicht dadurch einen organisationsübergreifenden Datenaustausch innerhalb des Gesundheitswesens.
TI Services	zentrale Dienste und Fachdienste der Telematikinfrastruktur
Trust-Service Status List (TSL)	Die Trust-service Status List enthält die öffentlichen Schlüssel aller vertrauenswürdigen CAs, die Information über den für diese CA akkreditierten Zertifikatstyp sowie die Adresse der Zertifikats Status Services (OCSP-Responder und CRL Provider). Sie ist durch gematik TSL Serviceprovider signiert.
Trusted Service Provider (TSP)	TSPs sind Stellen, die innerhalb oder im Auftrag der Teilnehmerorganisationen Zertifikate für natürliche oder juristische Personen oder technische Komponenten ausstellen und/oder Verzeichnisdienste betreiben.
Update-Daten	Update-Daten bestehen aus Updateinformation und Updatepaket, die gesondert integritätsgeschützt sind.
Verschlüsselungs-richtlinie	Verschlüsselungsrichtlinie, die beschreibt • das Verschlüsselungsformat (EncryptionType): Cryptographic Message Syntax [78] oder XML-Encryption [79] • für XML-Encryption: - XML-Schema: beschreibt die zu verschlüsselnden bzw. zu entschlüsselnden Daten,

	- Option: KeyInfo im XML-Dokument oder nicht • Herausgeber der Verschlüsselungsrichtlinie.
Vertrauensanker	Öffentlicher Schlüssel oder Zertifikat (in dem sich ein öffentlicher Schlüssel befindet), das als letzte Instanz bei der Prüfung einer Zertifikatskette in einer PKI zum Einsatz kommt. Dies kann bspw. der öffentliche Schlüssel eines Wurzel-Zertifikats (Root-CA) oder ein Signer-Zertifikat einer Liste von CAs (bspw. BnetzA-VL oder TSL) sein.
Vertrauensliste der Bundesnetzagentur (BnetzA-VL)	Vertrauensliste der Bundesnetzagentur mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die von der Bundesrepublik Deutschland beaufsichtigt werden, sowie mit Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten, vgl. eIDAS Artikel 22.
Vertrauensdienste-anbieter	„Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt, vgl. eIDAS [12] Artikel 3, Punkt 19.
VPN concentrator	VPN-Konzentrator
VPN-Konzentrator für den Zugang zur Telematikinfrastruktur	VPN-Konzentrator, welcher einen Zugang zur Telematikinfrastruktur bereitstellt – und damit auch einen Zugang für Dienste gemäß § 291 a SGB V (Pflichtanwendungen und freiwillige Anwendungen)
Zertifikat	Zertifikate sind elektronische Bescheinigungen, die von einer Zertifizierungsinstanz ausgestellt (signiert) werden, mit denen dem Zertifikatsinhaber bestimmte Informationen zugeordnet werden.
zu signierende Daten	Die Daten, deren Authentizität durch die elektronische Signatur geschützt werden soll und die von der SCaVA an die Signaturerstellungseinheit übergeben werden. Die Integrität der zu signierenden Daten ist zu schützen. Englisch: data to be signed, abgekürzt DTBS.
Zulässige Signaturrichtlinie	Eine Signaturrichtlinie ist zulässig, wenn sie für die Erzeugung qualifizierter elektronischer Signaturen die Benutzerinteraktion fordert und auf die zu signierenden Daten durch den EVG anwendbar ist. Die Installation der Signaturrichtlinie erfolgt mit der Installation oder Update des EVG oder der Fachanwendung, die diese Signaturrichtlinie implementiert.
Zulässige Verschlüs-selungsrichtlinie	Eine Verschlüsselungsrichtlinie ist zulässig, wenn die Regeln auf die zu verschlüsselnden oder zu entschlüsselnde Daten anwendbar sind. Die Installation der Verschlüsselungsrichtlinie erfolgt mit der Installation oder Update des EVG oder der Fachanwendung, die diese Verschlüsselungsrichtlinie implementiert.

Tabelle 41: Glossar

9.4. Abbildungsverzeichnis

9.5. Tabellenverzeichnis

9.6. Literaturverzeichnis

9.6.1. Kriterien

[4] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

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

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

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

[8] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[9] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[10] Joint Interprtation Library, Composite evaluation of Smart Cards and similar devices, January 2012, Version 1.2

[11] W. Killmann, W. Schindler: A proposal for: Functionality classes for random number generators. Version 2.0, September 2011

9.6.2. Gesetze und Verordnungen

[12] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG eIDAS-VO 2014

[13] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms Version 1.2 vom Januar 2020 https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

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

9.6.3. Schutzprofile und Technische Richtlinien

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

[16] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Version 1.6 vom 30.03.2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Version 1.6.6 vom 15.04.2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Technische Richtlinie TR-02102-3 Kryptographische Verfahren:Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Bundesamt für Sicherheit in der Informationstechnik, Version 2021-01

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

[20] Technische Richtlinie BSI TR-03144, eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Bundesamt für Sicherheit in der Informationstechnik, Version 1.2, 27.07.2017, Bundesamt für Sicherheit in der Informationstechnik

[21] BSI TR-03114 Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Protection Profile Electronic Health Card Terminal, BSI-PP-0032, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.10, 19.4.2013

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

[24] Technische Richtlinie BSI TR-03154, Konnektor – Prüfspezifikation für das Fachmodul NFDM, Version 1.1, 15.04.2019, Bundesamt für Sicherheit in der Informationstechnik

[25] Technische Richtlinie BSI TR-03155, Konnektor – Prüfspezifikation für das Fachmodul AMTS, Version 1.1, 15.04.2019, Bundesamt für Sicherheit in der Informationstechnik

[26] Technische Richtlinie BSI TR-03157, Konnektor – Prüfspezifikation für das Fachmodul ePA, Version 2.0.8, 02.05.2022, Bundesamt für Sicherheit in der Informationstechnik

9.6.4. Spezifikationen

[27] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor [gemSpec_Kon], PTV5: Version 5.15.0, 31.01.2022, gematik GmbH

[28] Elektronische Gesundheitskarte und Telematikinfrastruktur: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV5], Produkttyp Version: 5.1.0-0, Version 1.0.1, 10.02.2022, gematik GmbH

[29] Elektronische Gesundheitskarte und Telematikinfrastruktur: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik GmbH, Version 1.21.0, 21.01.2022

[30] Elektronische Gesundheitskarte und Telematikinfrastruktur - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt], gematik GmbH, Version 2.21.0, 31.01.2022

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

[32] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation der elektronischen Gesundheitskarte – eGK-Objektsystem [gemSpec_eGK_ObjSys], Version 3.13.0, 30.06.2021, gematik GmbH

[33] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation der gSMC-K / Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.13.0, 30.06.2021, gematik GmbH

[34] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation der gSMC-KT – Objektsystem [gemSpec_gSMC-KT_ObjSys], Version 4.2.0, 14.05.2018, gematik GmbH

[35] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation des elektronischen Heilberufsausweises – HBA-Objektsystem [gemSpec_HBA_ObjSys], Version 5.0.0, 10.09.2020, gematik GmbH

[36] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation der Security Module Card SMC-B Objektsystem [gemSpec_SMCB_ObjSys], Version 5.0.0, 10.09.2020, gematik GmbH

[37] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Fachmodul VSDM [gemSpec_FM_VSDM], Version 2.6.0, 12.11.2020, gematik GmbH

[38] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation eHealth-Kartenterminal [gemSpec_KT], Version: 3.14.0, Stand: 31.01.2022, gematik GmbH

[39] gestrichen

[40] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation TSL-Dienst [gemSpec_TSL]. Version 1.19.2, Stand 21.01.2022, gematik GmbH

[41] Elektronsiche Gesundheitskarte und Telematikinfrastruktur. Spezifikation Verzeichnisdienst [gemSpec_VZD]. Version 1.14.0, Stand 31.01.2022, gematik GmbH

[42] TeleTrusT: SICCT Secure Interoperable ChipCard Terminal, Version: 1.2.1, Date: 19.12.2010 mit ERRATA, Stand 12.9.2014, Version 1.0 Revision 1

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

[44] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Fachmodul NFDM [gemSpec_FM_NFDM], gematik GmbH, Version 1.6.2, 30.06.2021

[45] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Fachmodul AMTS [gemSpec_FM_AMTS], gematik GmbH, Version 1.4.0, 15.05.2019

[46] Signaturrichtlinie QES, Notfalldaten-Management (NFDM) [gemRL_QES_NFDM], gematik GmbH, Version 1.4.1, 02.03.2020

[47] Informationsmodell Notfalldaten-Management (NFDM) [gemSpec_InfoNFDM], gematik GmbH, Version 1.6.0, 02.03.2020

[48] Spezifikation Schlüsselgenerierungsdienst ePA [gemSpec_SGD_ePA], gematik GmbH, Version 1.4.2, 19.02.2021

[49] Spezifikation Fachmodul ePA [gemSpec_FM_ePA], gematik GmbH, Version 1.11.0, 31.01.2022

[50] Spezifikation Festlegung von OIDs [gemSpec_OID], gematik GmbH, Version 3.10.0, 19.02.2021

9.6.5. Standards

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

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

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

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

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

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

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

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

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

[60] C. Kaufman, P.Hoffman, Y.Nir, P.Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, RFC 7296 (IKEv2), http://www.ietf.org/rfc/rfc7296.txt

[61] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003, RFC 3602, http://www.rfc-editor.org/rfc/rfc3602.txt

[62] C. Madson, R. Glenn: Use of HMAC-SHA-1-96 within ESP and AH, November 1998, RFC 2404, http://www.rfc-editor.org/rfc/rfc2404.txt

[63] S. Kelly, S. Frankel: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. May 2007, RFC 4868, http://www.rfc-editor.org/rfc/rfc4868.txt

[64] T. Kivinen, M.Kojo: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). May 2003, RFC 3526, http://www.rfc-editor.org/rfc/rfc3526.txt

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

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

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

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

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

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

[71] Blake-Wilson, et al., Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), RFC 4492, May 2006

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

[73] R. Housley: Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, RFC 5083, November 2007, https://tools.ietf.org/html/rfc5083

[74] R. Housley: Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), RFC 5084, November 2007, https://tools.ietf.org/html/rfc5084

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

[76] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (May 2008), http://www.ietf.org/rfc/rfc5280.txt

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

[78] RFC 5652 (September 2009): Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc5652.txt

[79] XML Encryption Syntax and Processing, Version 1.1 W3C Recommendation, 11 April 2013, https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/

[80] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[81] XML Path Language (XPath) 2.0 (Second Edition), W3C Recommendation, 14 December 2010, https://www.w3.org/TR/2010/REC-xpath20-20101214/

[82] XML Advanced Electronic Signatures (XAdES), European Telecommunications Standards Institute (ETSI): Technical Specication XML Advanced Electronic Signatures (XAdES). ETSI Technical Specication TS 101 903, Version 1.4.2, 2010/

[83] XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 23 January 2007, https://www.w3.org/TR/2007/REC-xslt20-20070123/

[84] gestrichen

[85] ETSI: *Electronic Signature Formats*, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V1.7.4, 2008-07, via http://www.etsi.org

[86] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles, ETSI TS 102 778-3 V1.1.2, Technical Specification, 2009 2009

[87] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); XAdES Baseline Profile; ETSI Technical Specification TS 103 171, Version 2.1.1, 2012-03

[88] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); CAdES Baseline Profile; ETSI Technical Specification TS 103 173, Version 2.1.1, 2012-03

[89] European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); PAdES Baseline Profile; ETSI Technical Specification TS 103 172, Version 2.1.1, 2012-03

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

[91] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques. December 2001

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

[93] ISO/IEC 8859-15:1998 - 8-bit single-byte coded graphic character sets, Part 15: Latin alphabet No. 9, published March 15, 1999

[94] TIFF Revision 6.0, http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

[95] Unicode Standard Version 6.2.0. http://www.unicode.org/versions/Unicode6.2.0/

[96] ISO 19005 – Document management – Electronic document file format for long-term preservation

[97] ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)

[98] Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation 26 November 2008, https://www.w3.org/TR/xml/

[99] NIST 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[100] RFC 8422 (August 2018): Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier

[101] RFC 5639 (March 2020): Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, https://tools.ietf.org/html/rfc5639

[102] Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Certicom Research, Contact: Daniel R. L. Brown (dbrown@certicom.com), May 21, 2009, Version 2.0 https://www.secg.org/sec1-v2.pdf

[103] RFC 5869 (May 2010): HMAC-based Extract-and-Expand Key Derivation Function (HKDF), https://tools.ietf.org/html/rfc5869

[104] RFC 5116 (January 2008): An Interface and Algorithms for Authenticated Encryption, https://tools.ietf.org/html/rfc5116

[105] NIST 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[106] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/

[107] RFC 4122 (July 2005): A Universally Unique IDentifier (UUID) URN Namespace, https://tools.ietf.org/html/rfc4122

[108] NIST: FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[109] RFC 7027 (October 2013): Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), http://www.ietf.org/rfc/rfc7027.txt

9.6.6. Dokumentation

[110] secunet konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Bedienungsanleitung, Für Administratoren und Benutzer, Version 6.1, Secunet Security Networks AG

secunet konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Bedienungsanleitung, Für Administratoren und Benutzer, Version 6.1, Errata der Bedienungsanleitung, Version 1.0, 27.06.2022, Secunet Security Networks AG

[111] secunet konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Hinweise und Prüfpunkte für Endnutzer, Version 1.8, Secunet Security Networks AG

[112] secunet konnektor, Modularer Konnektor Version 2.0.0 und 2.1.0, Konnektor Management API-Dokumentation, Version 5.0.0, eHealth Experts GmbH

[113] secunet konnektor, Signaturdirektive, Secunet Security Networks AG, Version 1.50, 24.06.2022

[114] secunet konnektor, Dokumentensicherheit, Secunet Security Networks AG, Version 1.21, 17.05.2022

[115] secunet konnektor, Verschlüsselungsdirektive, Secunet Security Networks AG, Version 2.0, 21.06.2022

[116] secunet konnektor, Security Guidance Fachmodulentwicklung, Version 1.5, eHealth Experts GmbH