Security Target für RISE Konnektor V5.0

Release, basierend auf Schutzprofil BSI-CC-PP-0098-V3

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F
2320 Schwechat
Austria (Europe)
Tel: +43 1 9049007-0
E-Mail: welcome@rise-world.com
Internet: https://www.rise-world.com

Änderungsverlauf

Version	Datum	Änderungen	Anmerkungen
0.4	14.04.2020	Ausgehendend vom ST für PTV3 Version 0.91: Anpassung an PTV4 Ergänzung SFR für VAU-Kommunikation und SGD-Kommunikation sowie Anforderungen an die ECC-Migration	Version für PTV4 zur Vorlage bei der gematik und BSI.
0.5	08.06.2020	Kommentierung gematik eingearbeitet; redaktionelle Korrekturen	
0.6	29.06.2020	Erneute Kommentierung gematik eingearbeitet	
0.7	25.11.2020	Einarbeitung Hinweise BSI	
0.8	08.01.2021	Hinweise Prüfstelle eingearbeitet	Inkl. Anpassung an PP-0098-V3, Version 1.5.7 vom 18.12.2020 Inkl. Hinweise gematik bzgl. unterstützter Karten im SGD-Protokoll
0.9	15.01.2021	Weitere Hinweise Prüfstelle eingearbeitet, Redaktionelle Korrekturen	
1.0	19.01.2021	Redaktionelle Korrekturen	
1.1	20.01.2021	Redaktionelle Korrekturen	Version für PTV4 zur Vorlage bei gematik und BSI
1.2	13.04.2021	• Korrektur Signaturhashalgorithmen • Anpassungen SGD-Protokoll • BSI-Kommentierung bearbeitet • Versionanpassung Firmware	Version für PTV4 zur Vorlage bei gematik und BSI
1.3	15.04.2021	Änderung des unterliegenden PP eingepflegt	Version für PTV4 zur Vorlage bei gematik und BSI
1.31	21.04.2021	• Formulierung zu Anwendungshinweis 89 korrigiert. • Redaktionelle Korrekturen	Version für PTV4 zur Vorlage bei gematik und BSI
1.4	28.04.2021	Änderung des unterliegenden PP eingepflegt	Version für PTV4 zur Vorlage bei gematik und BSI
1.5	18.05.2021	Ergänzung in FCS_COP.1/NK.TLS.Auth	Version für PTV4 zur Vorlage bei gematik und BSI
2.0	08.06.2021	Erweiterung um prüfungsrelevante Sicherheitsfunktionen im Kontext der Komfortsignatur	PTV 4.0+ abgestimmt mit gematik

Version	Datum	Änderungen	Anmerkungen
2.1	20.07.2021	Anpassungen an PTV5	
2.2	10.08.2021	Einarbeitung Hinweise der Prüfstelle	
2.3	23.08.2021	Weitere Hinweise der Prüfstelle eingearbeitet	
2.4	29.08.2021	Ergänzung in FIA_UAU.5/AK Redaktionelle Anpassungen	
2.5	09.09.2021	Korrekturen in 8.5, Aufnahme O.AK.Sig.Komfortsignatur und Ergänzung OE.AK.Clientsystem, Ergänzung Kap. 6.5.8 zur Komfortsignatur	
2.6	22.09.2021	Redaktionelle Anpassungen	
2.7	23.09.2021	Formatänderungen	Version für PTV5 zur Vorlage bei gematik und BSI
3.0	10.01.2022	Korrekturen in 8.5 bzgl. A_19052 Anpassung FCS_COP.1.1/SGD.ECIES, Hinweis 4 Redaktionelle Anpassungen	Inkl. Anpassungen in Anwendungshinweis 142: und Anwendungshinweis 143: sowie Anwendungshinweis 137: und Anwendungshinweis 134: Version für PTV5 zur Vorlage bei gematik und BSI
3.1	17.01.2022	Weitergabehinweis entfernt	Version für PTV5 zur Veröffentlichung durch BSI geeignet

Inhaltsverzeichnis

1. ST-Einführung

1.1. ST und EVG Referenz

Titel:	Security Target für RISE Konnektor V5.0
ST Version:	3.1
ST Datum:	17.01.2022
Allgemeiner Status:	Release, basierend auf Schutzprofil BSI-CC-PP-0098-V3
Zertifizierungs ID:	BSI-DSZ-CC-1189
PP Registrierung bei:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC-Version	3.1 (Revision 5)
Vertrauenswürdigkeitsstufe:	EAL3 erweitert um AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 und ALC_FLR.2
Hersteller:	Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Name des EVG	RISE Konnektor
EVG Version[1]	V5.0
Stichwörter:	Konnektor, Anwendungskonnektor, eHealth, elektronisches Gesundheitswesen, Telematikinfrastruktur, dezentrale Komponente

Dieses Dokument orientiert sich in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang in Abschnitt 9.6 (insbesondere Abschnitt 9.6.5) aufgeführt sind; allen voran die Konnektorspezifikation:

[93] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor, Version 5.14.0, 02.09.2021, gematik GmbH

[1] Vgl. Tabelle 1 für Versionsnummern von Teilkomponenten.

1.2. EVG-Übersicht

Das Security Target beschreibt und begründet die Sicherheitsanforderungen an den Konnektor gemäß Spezifikation [92]. Der Konnektor ist darauf ausgerichtet, durch Weiterentwicklung und Update im Feld langfristig genutzt zu werden.

Der Konnektor enthält die Funktionsblöcke Netzkonnektor (NK) und dem Anwendungskonnektor (AK) und benötigt die Security Module Card Konnektor (gSMC-K). Er stellt die Plattform für die Ausführung von Fachmodulen bereit.

Die Sicherheitsanforderungen an die Sicherheitsfunktionalität des Netzkonnektors sind, wenn dieser als Einzelkomponente evaluiert wird, im Schutzprofil BSI-CC-PP-0097-V2 beschrieben. Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssystem und dem Objektsystem für gSMC-K, welche von der gematik zugelassen sind. Es speichert Schlüsselmaterial für den Konnektor und stellt kryptographische Sicherheitsfunktionen in der Einsatzumgebung bereit.

Die Sicherheitsfunktionalität des Konnektors umfasst die Paketfilter- und VPN-Funktionalität für die Kommunikation mit der zentralen Telematikinfrastruktur-Plattform und einem Sicheren Internet Service (SIS), einer SCaVA (Signature Creation Application and Signature Validation Application), die Verschlüsselung und Entschlüsselung von Dokumenten, den Kartenterminaldienst, den Chipkartendienst, die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem sowie zwischen Fachmodulen und Fachdiensten.

1.2.1. Abgrenzung

Das vorliegende Security Target definiert die Sicherheitsanforderungen an den Gesamtkonnektor, wie er im Schutzprofil BSI-CC-PP-0098-V3 abgegrenzt ist.

Das Chipkartenbetriebssystem der gSMC-K ist von der gematik zugelassen (A.AK.gSMC-K). Für das Chipkartenbetriebssystem der gSMC-K existiert eine eigene Spezifikation [97].

1.2.2. Terminologie

Zum zugrundliegenden Schutzprofil konforme EVGs werden als Konnektor bezeichnet.

Der Konnektor bildet die Schnittstelle zwischen der zentralen Telematikinfrastruktur-Plattform des Gesundheitswesens[2] und den Clientsystemen des Gesundheitswesens. Die Chipkarten elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA), die Institutskarte (SMC-B, Security Module Card Typ B), die SMC-B der Gesellschafterorganisationen (SMC-B ORG), der 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

[2] Ein Glossar der wichtigsten Begriffe befindet sich im Anhang. Für Fachtermini der elektronischen Gesundheitskarte und der Telematikinfrastruktur des Gesundheitswesens wird darüber hinaus auf die Seiten des Bundesministeriums für Gesundheit (BMG, http://www.bmg.bund.de), der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik, http://www.gematik.de) und des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI, http://www.dimdi.de) verwiesen.

die Apothekenverwaltungssysteme (AVS). Der Konnektor stellt auch eine gesicherte Verbindung zu einem Sicheren Internet Server (SIS) bereit. Der Konnektor unterstützt weiterhin die Vorläuferkarten des HBA, den HBA-qSig und den ZOD-2.0.

Anmerkung: SM-B ist ein Zusammenfassender Begriff für eine SMC-B (Security Module Card Typ B, „Institutionskarte"), als auch eine in einem HSM-B (HSM-Variante einer Security Module Card Typ B) enthaltene virtuelle SMC-B verwendet. Die Verwendung eines HSM-B ist nur dann zulässig, wenn die Umgebungsanforderungen daran erfüllt werden. Funktional entspricht das HSM-B einer bzw. mehrerer SMC-Bs. Im Folgenden werden die Begriffe SMC-B und SM-B synonym verwendet.

HBAx ist ein Zusammenfassender Begriff für den HBA sowie die Vorläuferkarten des HBA, den HBA-qSig und den ZOD-2.0. Immer dann, wenn die Funktionalität des HBA auch durch die Vorgängerkarten geleistet werden kann, ist es zulässig ein HBAx zu verwenden.

Zur Verwendung der Begriffe VSDM Fachdienst und VSDM Intermediär siehe Anwendungshinweis 1.

Audit-Daten vs. Logging: Der Begriff Audit-Daten wird in diesem Security Target auch im Sinne der Common Criteria verwendet. Im Sinne der Common Criteria bezeichnet dieser Begriff ganz allgemein Anforderungen aus der Klasse FAU (Security Audit) aus Common Criteria Teil 2 [2], die im Gesundheitswesen eher mit „Logging" bezeichnet würden. Dieses Security Target verwendet ebenfalls den Begriff „Logging", wo dies möglich ist, nutzt aber auch den Begriff „Audit", wenn z. B. funktionale Anforderungen aus den Common Criteria zitiert werden. Die Funktionalität, die üblicherweise unter dem Begriff „Audit" verstanden wird, wird hier durch O.AK.Protokoll gefordert.

1.3. EVG-Beschreibung

Der Evaluierungsgegenstand (EVG) ist der Konnektor [92] gemäß der Abgrenzung in BSI-CC-PP-0098-V3 und umfasst folgende Anteile:

- Software des Netzkonnektors;
- Software des Anwendungskonnektors;
- Software des Fachmoduls VSDM.

Die folgenden Konnektoranteile sind nicht Bestandteil des EVG:

- Hardware inkl. BIOS;
- Software des Fachmoduls AMTS;
- Software des Fachmoduls NFDM.
- Software des Fachmoduls ePA

Der Konnektor wird als eine Einbox-Lösung implementiert. Das Gerät, das den EVG beinhaltet, ist in einem quaderförmigen Gehäuse untergebracht, und verfügt über die Hardwareanschlüsse, die für den Betrieb des Konnektors nötig sind. Die gSMC-Ks (vgl. Abschnitt 1.3.6) befinden sich ebenfalls in diesem Gehäuse.

Der EVG RISE Konnektor V5.0 besteht aus folgenden Teilkomponenten und wird ausschließlich mit der genannten Hardwareversion ausgeliefert:

Komponenten	Version
Software des Konnektors (inkl. Fachmodul VSDM)	4.2.8
Fachmodul AMTS *(nicht Teil des EVG)*	1.1.1
Fachmodul NFDM *(nicht Teil des EVG)*	1.1.1
Fachmodul ePA *(nicht Teil des EVG)*	2.0.0
Hardware inkl. BIOS (nicht Teil des EVG)	*1.0.0*

Tabelle 1: Komponenten der Einbox-Lösung

Das Gerät wird über eine Lieferkette dem Endkunden (Leistungserbringer) zugestellt. Die Sicherheit der Lieferkette wird durch die Vertrauenswürdigkeitskomponente ALC_DEL.1 gewährleistet, vgl. auch Abschnitt 6.4.4. Die Anweisungen an den Nutzer, wie die Einhaltung der sicheren Lieferkette überprüft werden kann, sind auch im Benutzerhandbuch enthalten.

Der Lieferumfang des EVG umfasst ebenfalls die Betriebsdokumentation für den Konnektor:

- RISE Konnektor Bedienungsanleitung, [RISE-KON-AGD_OPE];

Im Zertifizierungsreport, der nach Abschluss der Evaluierung ebenso wie diese Sicherheitsvorgaben auf der Internetpräsenz[3] des Bundesamts für Sicherheit in der Informationstechnik (BSI) veröffentlicht wird, ist der Hashwert des Handbuchs genannt. Dieser Hashwert gibt dem Endkunden die Möglichkeit, die Integrität und Authentizität des Handbuchs zu verifizieren.

1.3.1. EVG Typ

Der vorliegende Konnektor stellt einen neuen Produkttyp gemäß [91] dar, sodass außer dem Gattungsbegriff „Konnektor“ kein weiterer Typ benannt werden kann.

Der Konnektor umfasst die Sicherheitsfunktionalität einer Firewall, eines VPN-Clients, einer SCaVA, eines Kryptomoduls für Verschlüsselung und gesicherte Kommunikation sowie von Servern für Kartenterminaldienste, Chipkartendienste, Zeitdienst, DNS und DHCP-Dienst.

Die Sicherheitsfunktionalität einer Firewall, eines VPN-Clients, und von Servern für Zeitdienst, DNS und DHCP-Dienst werden durch den Bestandteil Netzkonnektor erbracht. Die Sicherheitsfunktionalität einer SCaVA, eines Kryptomoduls für die Verschlüsselung und die gesicherte Kommunikation zwischen dem Konnektor und dem Clientsystem, zwischen Fachmodulen und Fachdiensten sowie zwischen Servern und dem Kartenterminaldienst, dem Chipkartendienst, werden durch den Anwendungskonnektor erbracht. Zur Absicherung der Kommunikation verwendet der Anwendungskonnektor die TLS-Dienste, die vom Netzkonnektor bereitgestellt werden.
Das Sicherheitsmodul gSMC-K stellt Sicherheitsfunktionalität zur Speicherung von

[3] https://www.bsi.bund.de/

Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit.

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

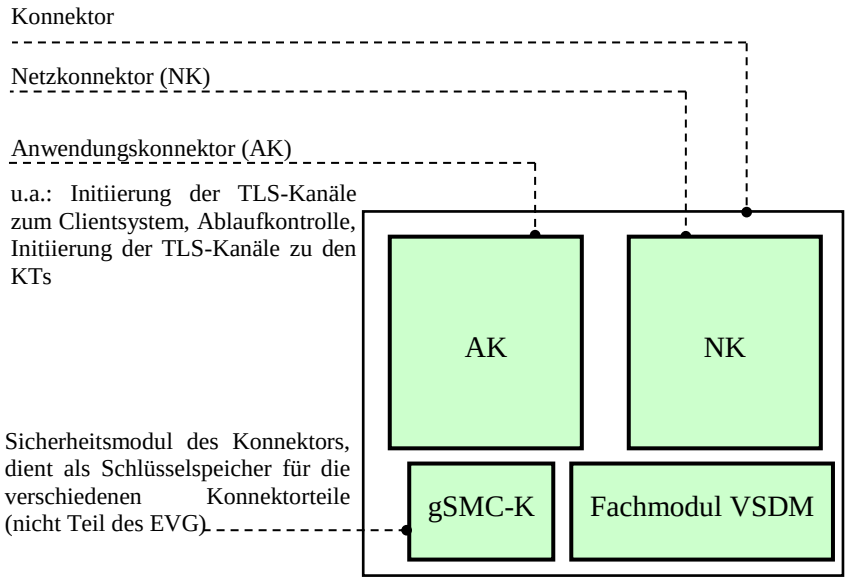


Abbildung 1: Funktionsblöcke des Konnektors

Im Folgenden werden die einzelnen Funktionalitäten kurz vorgestellt:

Firewall

Der Konnektor 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 Konnektor als Internet Gateway und stellt einen sicheren Kanal zum Zugangspunkt des sicheren Internet-Dienstleisters sowie einen Paketfilter (IP-Firewall) zur Verfügung.

VPN-Client

Der Konnektor baut mit einem VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform einen VPN-Kanal gemäß dem Standard IPsec (IP Security) auf. Konnektor 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 Konnektor Schlüsselmaterial, welches auf einem dem Konnektor zugeordneten Sicherheitsmodul (gSMC-K) gespeichert ist.

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

Der VPN-Kanal zum VPN-Konzentrator der zentralen Telematikinfrastruktur-Plattform für die Kommunikation mit der Telematikinfrastruktur stellt eine Absicherung der Kommunikationsbeziehung zwischen Konnektor und VPN-Konzentrator auf Netzwerkebene dar. Nach erfolgtem Aufbau des VPN-Tunnels zur Telematikinfrastruktur durch den Konnektor wird dieser Kanal genutzt und authentisiert[4] die Organisation des Leistungserbringers gegenüber den Fachdiensten. Dazu nutzt der Konnektor Schlüsselmaterial, welches auf einem der Organisation des Leistungserbringers zugeordneten Sicherheitsmodul (SM-B) gespeichert ist.

TLS-Kanal

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

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

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.

[4] Diese Authentisierung ist nicht Gegenstand der vorliegenden Sicherheitsvorgaben.

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 [46] und RFC 2132 [47] zur Verfügung.

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 [8] 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 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 [75]). Der Signaturdienst unterstützt darüber hinaus die Erstellung von qualifizierten Einfachsignaturen (s.a. [75]) 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).

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 oder dem VSDM Fachmodul 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 [92] zur Verfügung und erbringt Sicherheitsfunktionalität für deren sichere Nutzung und den Schutz der Ressourcen.

Der EVG kommuniziert mit den eHealth-Kartenterminals (eHKT, s. [94]) 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 [95].

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 den Fachdienst VSDM.

Unterstützung des zentralen Verzeichnisdienstes

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

1.3.2. Einsatzumgebung

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.AK.phys_Schutz). Die Betriebsumgebung des EVG ist ein geschützter Einsatzbereich.

Die Einsatzumgebung des EVG als Einbox-Lösung ist in der folgenden Abbildung 2 schematisch dargestellt. Insbesondere wird der Konnektor immer mit den Komponenten Anwendungskonnektor, Netzkonnektor und gSMC-K gemeinsam betrieben, wobei die gSMC-K durch die gematik zugelassen wurde.

Die in Abbildung 2 links vom Transportnetz dargestellten Komponenten befinden sich im lokalen Netz der Leistungserbringer und werden als dezentrale Komponenten bezeichnet. Die VPN-Konzentratoren und die übrigen rechts bzw. unterhalb vom Transportnetz dargestellten Dienste mit Ausnahme der Fachdienste werden als zentrale Dienste oder zentrale Telematikinfrastruktur-Plattform bezeichnet.

Alle Teilkomponenten des EVG sind durch dicke schwarze Rahmen und blaue Einfärbung gekennzeichnet. Mit roten Linien werden zum besseren Verständnis Komponenten zusammengefasst, die üblicherweise in einem gemeinsamen Gehäuse untergebracht sind (insbesondere bei der Einbox-Lösung) oder die auf einer gemeinsamen Plattform ablaufen (z. B. Hardware des Clientsystems). Abhängig vom Einsatzszenario können die roten Linien geschützten Bereichen (vgl. A.AK.phys_Schutz) entsprechen. Die gezeichneten (schwarzen) Verbindungslinien kennzeichnen die physischen Verbindungen der entsprechenden Komponenten.

Anwendungshinweis 2: Zusätzlich zu den in BSI-CC-PP-0098-V3 geführten Komponenten der Einsatzumgebung werden in diesem Security Target die Fachmodule NFDM, AMTS und ePA als Teil der Einsatzumgebung betrachtet. Die Fachmodule sind Teile der Einbox-Lösung wie in Abbildung 2 und Abbildung 5 schematisch dargestellt. Die Einsatzumgebung wird im Übrigen unverändert aus BSI-CC-PP-0098-V3 übernommen und um die logischen Schnittstellen zur VAU bzw SGD ergänzt.

In Abbildung 2 bedeuten die Abkürzungen (siehe auch Kapitel 9.1):

- NK: Netzkonnektor
- EVG: Evaluierungsgegenstand
- AK: Anwendungskonnektor
- KT (= eHealth KT): Kartenterminal im Gesundheitswesen; in der Abbildung ist aus Gründen der Übersichtlichkeit 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 Organisation
- gSMC-K: Sicherheitsmodul des Konnektors (nicht Teil des EVG)
- SIS: Sicherer Internet Service
- TI: Telematikinfrastruktur
- VSDM: Versichertenstammdatenmanagement
- VSDD: Versichertenstammdatendienst
- AMTS: Arzneimitteltherapiesicherheit
- NFDM: Notfalldatenmanagement
- ePA: elektronische Patientenakte

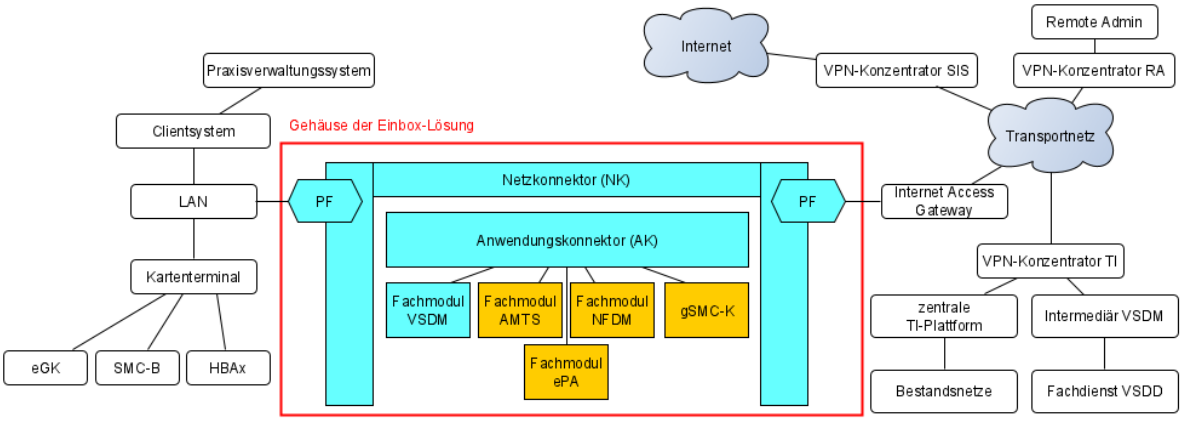


Abbildung 2: Einsatzumgebung des Konnektors

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

In Abbildung 3 sind die logischen Kanäle, an denen der EVG beteiligt ist, symbolisch dargestellt. Aus Gründen der Übersichtlichkeit wurden die zugrunde liegenden physischen Verbindungen nicht gezeichnet. Zur Interpretation der zu nutzenden physischen Verbindungen ist daher Abbildung 2 einzubeziehen. Die logischen Kanäle, die im Zusammenhang mit der Nutzung des Fachmoduls ePA entstehen sind aus Gründen der Übersichtlichkeit in Abbildung 4 dargestellt und anschließend beschrieben.

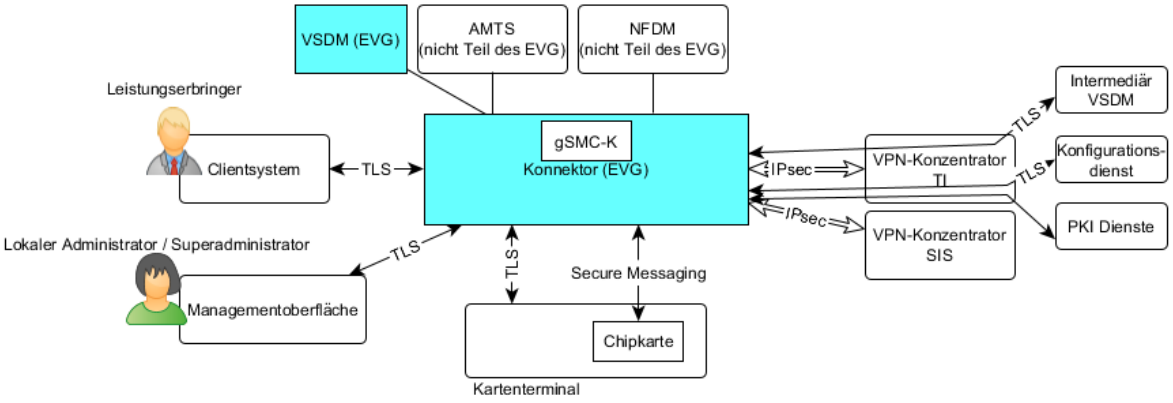


Abbildung 3: Logische Kanäle des EVG in seiner Einsatzumgebung

Im Folgenden werden die Komponenten der Einsatzumgebung vorgestellt, mit denen der EVG zusammenarbeitet:

gSMC-K

Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssystem und dem Objektsystem für gSMC-K, welche von der gematik zugelassen sind. Es speichert Schlüsselmaterial für den Netzkonnektor und den Anwendungskonnektor und stellt kryptographische Sicherheitsfunktionen bereit

Clientsystem im lokalen Netz des Leistungserbringers

Ein IT-System, das bei einem Leistungserbringer eingesetzt wird – z.B. eine Praxisverwaltungssoftware (PVS), ein Krankenhausinformationssystem (KIS) oder eine Apothekensoftware (AVS) – und sich unter dessen administrativer Hoheit befindet. Das Clientsystem nutzt die Dienstleistungen des Konnektors und der Fachmodule für die Kommunikation mit den Fachdiensten sowie optional mit dem Internet[5].

eHealth-Kartenterminals

Die eHealth-Kartenterminals sind gemäß Schutzprofil [80] evaluiert. Der EVG kommuniziert mit den eHealth-Kartenterminals über SICCT-Kommandos gemäß Spezifikation [94] [96] in TLS-Kanälen, die die Vertraulichkeit und Integrität der Kommunikation schützen. Die SICCT-Kommandos dienen

- der Steuerung des eHealth-Kartenterminals, insbesondere der Kommunikation mit dem Konnektor, der Kommandoausführung und der Konfiguration des eHealth-Kartenterminals, die nicht durch die folgenden Punkte erfasst werden,
- dem Zugriff auf die Anzeige (Display und Anzeige des gesicherten PIN-Modus), und die Tastatur sowie dem optionalen Tongeber,
- der Kontrolle, Aktivierung, Deaktivierung und Statusabfrage des elektrischen Zustands von Chipkartenkontaktiereinheiten,

[5] Abhängig von der Netzwerk-Konfiguration kann der Zugriff zum Internet über den sicheren Tunnel zwischen Konnektor und SIS erfolgen oder über ein anderes, sicheres Gateway, siehe Kapitel 2.7 in [**Fehler! Textmarke nicht definiert.**].

- der Kommunikation mit Chipkarten in den Chipkartenslots, und
- die Auslösung der Prozesse zur PIN-Eingabe und dem PIN-Wechsel im gesicherten Modus.

Der EVG identifiziert die eHealth-Kartenterminals und authentisiert sie anhand ihrer Zertifikate beim Aufbau des TLS-Kanals und eines Pairing-Geheimnisses aus einem Pairing-Prozess, siehe [94], Kapitel 3.7. Der EVG ordnet die mit ihm gepaarten eHealth-Kartenterminals den Arbeitsplätzen zu.

Jedes eHealth-Kartenterminal erzwingt die Nutzung genau eines TLS-Kanals für die Nutzung mit den gesteckten Chipkarten. Für den Aufbau des TLS-Kanals enthält jedes eHealth-Kartenterminal eine gSMC-KT oder nutzt eine SMC Typ B. Das eHealth-Kartenterminal informiert den EVG über alle Chipkartenoperationen, wie z. B. Chipkarte gesteckt oder Chipkarte entnommen.

In den eHealth-Kartenterminals stecken eine oder mehrere benutzte Chipkarten[6] HBA, eGK, bzw. SMC-B für die Erzeugung qualifizierter elektronischer Signaturen, digitaler Signaturen oder die Entschlüsselung von Dokumentenschlüsseln. Der EVG unterstützt auch die Nutzung von KVK in den eHealth-Kartenterminals.

Der EVG verwendet eHealth-Kartenterminals als PIN-Terminal und als Chipkarten-Terminal.

Die PIN-Terminals dienen der entfernten oder lokalen Eingabe der PIN. Die Benutzer geben ihre Authentisierungsverifikationsdaten (PIN oder PUK) an PIN-Terminals

- lokal ein (*lokale PIN-Eingabe*, vergl. [75]), d.h. die Eingabe erfolgt an dem Chipkartenterminal, im dem die Chipkarte gesteckt ist, die diese PIN bzw. PUK prüft, oder
- entfernt ein (*entfernte PIN-Eingabe*, vergl. [75]), d.h. die Eingabe erfolgt an einem anderen Chipkartenterminal, das verschieden ist von dem Kartenterminal, in welchem sich die Chipkarte befindet, die die PIN bzw. PUK prüft.

Der EVG steuert die Abläufe der PIN-Terminals für die lokale und entfernte PIN-Eingabe über SICCT-Kommandos, insbesondere die Anzeige für die Eingabe der PIN, die gesicherte PIN-Eingabe bei der lokalen PIN-Eingabe und die gesicherte Übertragung an die Chipkarte bei der entfernten PIN-Eingabe.

Chipkarten

Der EVG identifiziert und authentisiert Chipkarten eGK, HBA und SMC-B vor ihrer Benutzung[7] und arbeitet nur mit Chipkarten zusammen, die gemäß den relevanten Schutzprofilen evaluiert und zertifiziert sind. Der EVG unterstützt darüber hinaus reduzierte

[6] Die eHealth-Kartenterminals besitzen mehrere, durch SICCT-Kommandos einzeln adressierbare Slots zur Aufnahme von Chipkarten.

[7] Die Authentisierung der Chipkarten ist notwendig, um einen Nachweis für die angegebene Identität der Chipkarte und ihre vom EVG genutzte Funktionalität zu erhalten.

Funktionalität der KVK. Der EVG benutzt bzw. unterstützt die Nutzung der Chipkarten in der Einsatzumgebung des Leistungserbringers wie folgt:

- Eine eGK dient als Träger der Versichertenstammdaten und Daten der Gesundheitsanwendungen, kryptographischer Schlüssel und Zertifikate für die Verschlüsselung, und Authentisierung sowie als PIN-Empfänger für die Kartenhalter-PIN.
- Ein HBA dient als qualifizierte Signaturerstellungseinheit, als Träger des Entschlüsselungsschlüssels, von Zertifikaten sowie als PIN-Empfänger für die Signatur- und die Kartenhalter-PIN.
- Eine SMC-B dient als Träger eines Signaturschlüssels, eines Entschlüsselungs-schlüssels, von Zertifikaten und als PIN-Empfänger.
- Ein HBA und eine SMC-B dienen als Gegenstelle der Card-to-Card-Authentisierung gegenüber der eGK zum Nachweis der Einsatzumgebung der eGK.
- Die gSMC-KT dient als PIN-Sender, Endpunkt eines Secure Messaging[8] Kanals und als Träger des privaten Schlüssels und des Zertifikats für einen TLS-Kanal zwischen einem eHealth-Kartenterminal und dem EVG.

Die Kommunikation des EVG erfolgt mit den Chipkarten innerhalb des TLS-Kanals mit den eHealth-Kartenterminals im Klartext oder mit dem HBA auch in einem Secure Messaging Kanal der gSMC-K [75]. HBA und SMC-B verfügen über unterschiedliche Zertifikate und Schlüsselmaterial des Kartenhalters entsprechend dessen Befugnissen insbesondere gegenüber den eGK.

VPN Konzentrator der zentralen Telematikinfrastruktur-Plattform (TI-Plattform)

Der VPN-Konzentrator der zentralen TI-Plattform dient als VPN-Gateway und damit als Tunnel-Endpunkt einer geschützten Kommunikation vom bzw. zum EVG über das Transportnetz. Diese Kommunikation ist durch IPsec bezüglich Vertraulichkeit und Integrität geschützt, siehe Kapitel 1.3.1 in [77] (VPN-Client). Der damit verfügbare sichere Kanal verbindet das lokale Netz des Leistungserbringers mit der zentralen Telematikinfrastruktur-Plattform. Dadurch wird ein sicherer Zugriff des EVG auf die Fachdienste ermöglicht. Ferner können Clientsysteme auch auf die Dienste der Bestandsnetze zugreifen.

VPN Konzentrator des Sicheren Internet Servers (SIS)

Der VPN-Konzentrator des SIS dient als VPN-Gateway und damit als Tunnel-Endpunkt einer geschützten Kommunikation vom bzw. zum EVG über das Transportnetz. Diese Kommunikation ist durch IPsec bezüglich Vertraulichkeit und Integrität geschützt, siehe Kapitel 1.3.1 in [77] (VPN-Client). Der damit verfügbare sichere Kanal verbindet das lokale Netz des Leistungserbringers mit Systemen aus dem Internet. Zur Sicherung der Systeme im lokalen Netz der Leistungserbringer vor Angriffen aus dem Internet sind auf dem SIS weitere Schutzmaßnahmen installiert (siehe OSP.NK.SIS).

[8] Secure Messaging ermöglicht eine verschlüsselte und MAC-gesicherte Kommunikation

Fachdienste und Fachmodule

Der EVG ermöglicht es Fachmodulen auf Fachdienste zuzugreifen. Dazu dient er als Kommunikationsendpunkt für die sichere Kommunikation mit den Fachdiensten. Dazu werden vom EVG auf Anforderung der Fachmodule entsprechende TLS-Kanäle auf- und abgebaut. Außerdem bietet der EVG den Fachmodulen kryptographische Dienstleistungen an.

PKI Dienste

Der EVG nutzt OCSP-Dienste als PKI-Dienstleistung der TI für die Prüfung von Zertifikaten bei der Erstellung qualifizierter elektronischer Signaturen und der Prüfung qualifizierter und nicht-qualifizierter elektronischer Signaturen, dem Aufbau gesicherter Kommunikationskanäle sowie dem Verschlüsseln von Daten.

Darüber hinaus werden TSL, CRL und BNetzA-VL Daten zum Download bereitgestellt, die vom EVG zur Prüfung von Zertifikaten herangezogen werden.

Konfigurationsdienst

Der Konfigurationsdienst stellt für den Konnektor und für eHealth-Kartenterminals Software-Updates bereit. Darüber hinaus stellt er für den Konnektor zentrale Konfigurationsdaten zur Anbindung von Bestandsnetzen bereit.

Kommunikation ePA

Durch die Einführung des Fachmoduls ePA entstehen zwei zustätzliche logische Kanäle, die aus Gründen der besseren Übersichtlichkeit in der nachvolgenden Abbildung 4 dargestellt und deren Elemente anschließend beschrieben sind, sofern dies nicht im vorangegangenen Text erfolgt ist.

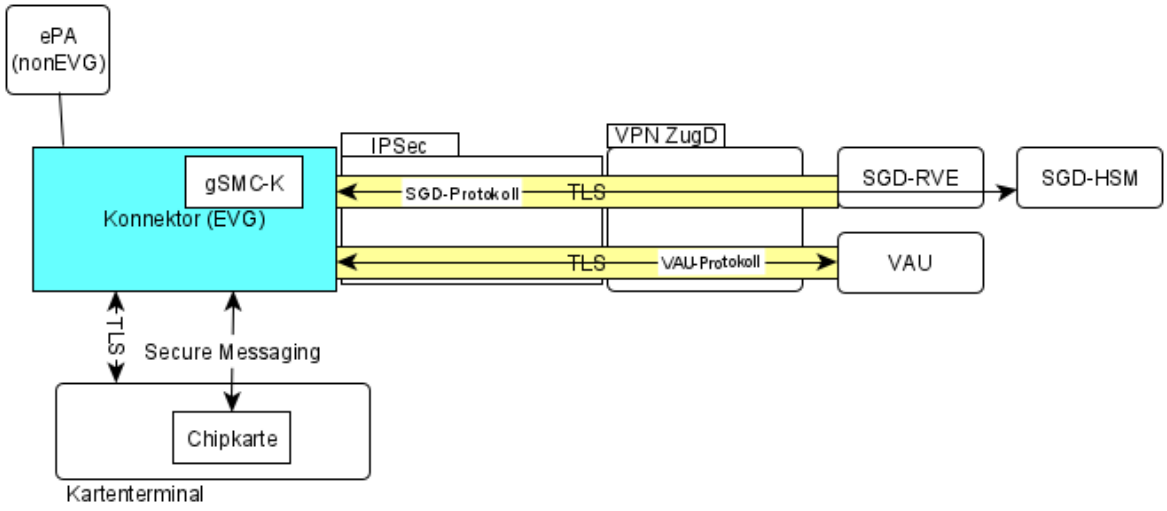


Abbildung 4: Logische Kanäle des EVG im Zusammenhang mit ePA

SGD-HSM

Im Rahmen des Zugriffes auf die ePA ruft das FM ePA Schlüssel aus dem Schlüsselgenerierungsdienst (SGD) ab um entweder Daten für den richtigen Empfänger verschlüsseln oder Daten entschlüsseln zu können. Für die Kommunikation mit dem HSM des

SGD und zum Schutz des Schlüsselmaterials wird eine eigene Sicherungsschicht „SGD-Kommunikation“ eingeführt.

SGD-RVE

Die Requestverarbeitende Einheit des SGD (SGD-RVE) bildet den Endpunkt der TLS-Verbindung zwischen ePA Client (hier: Fachmodul ePA) und dem SGD.

VAU

VAU ist die Vertrauenswürdige Ausführungsumgebung des ePA Dokumentensystems. Um die VAU sicher auch aus einem mobilen Szenario ansprechen zu können, in dem kein Konnektor vorhanden ist, wurde die VAU-Kommunikation eingeführt. Im hier vorliegenden Fall der Nutzung eines Konnektors mit ePA Fachmodul erfolgt die VAU-Kommunikation innerhalb eines TLS-Kanals zwischen Konnektor und dem ePA Aktensystem (Endpunkt: VAU).

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 3: Der EVG unterstützt alle von BSI-CC-PP-0097-V2 und BSI-CC-PP-0098-V3 erwarteten physischen Schnittstellen und implementiert darüber hinaus die herstellerspezifische Schnittstelle PS4 wie im Folgenden dargestellt.

Der EVG besitzt folgende physische Schnittstellen:

PS1 Eine Schnittstelle zum LAN bzw. zum Clientsystem.

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

PS2 Eine Schnittstelle zu Datennetzen (WAN), welche als Transportnetz für den Zugang zur Telematikinfrastruktur und ggf. zum Internet dienen. Es wird angenommen, dass diese Datennetze möglicherweise öffentlich zugänglich und Verbindungen mit ihnen nicht notwendigerweise verschlüsselt sind.[9]

Anwendungshinweis 4: Durch die für dieses ST relevante Einboxlösung des Konnektors ist die Identifizierung einer physischen Schnittstelle zwischen Netzkonnektor und dem Anwendungskonnektor nicht erforderlich. In diesem ST wird die Nummerierung aus dem PP BSI-CC-PP-0098-V3 beibehalten. Die mit PS1 bezeichnete LAN-Schnittstelle und die mit PS2 bezeichnete WAN-Schnittstelle fallen nicht in einer physischen Schnittstelle zusammen, da getrennte Netzwerkcontroller verwendet werden.

PS3 Eine Schnittstelle zum Sicherheitsmodul des Netzkonnektors (gSMC-K). Das Sicherheitsmodul gSMC-K stellt Sicherheitsfunktionalität zur Speicherung

[9] In der Konnektorspezifikation [**Fehler! Textmarke nicht definiert.**] sind Szenarien definiert, die für eine Verbindung zum Transportnetz die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

von Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit.
Die gSMC-K ist sicher mit dem EVG verbunden. Siehe auch OE.NK.gSMC-K.

PS4 Eine Schnittstelle zur Signaleinrichtung (Signalisierung).
Der Konnektor verfügt über drei LEDs zur Anzeige von Statusmeldungen (Power, Verbindungsstatus, Fehlerzustand).

Schließlich wird die physische Hülle des Konnektors als weitere Schnittstelle betrachtet. Aufgrund der Annahme A.AK.phys_Schutz werden keine Angriffe über diese Schnittstelle betrachtet. Abbildung 5 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 [77].

Anwendungshinweis 5: Die Schnittstellen sind in Abbildung 2 und Abbildung 5 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 BSI-CC-PP-0098-V3 [78] sind enthalten. Der EVG implementiert darüber hinaus die herstellerspezifische Schnittstelle LS13 wie im Folgenden dargestellt.
Abweichend vom BSI-CC-PP-0098-V3 [78] wird die Schnittstelle zum Fachmodul VSDM nicht als logische Schnittstelle geführt, da es sich hierbei um EVG-interne Kommunikation handelt.

Der EVG besitzt folgende (externe) logische Schnittstellen (siehe auch Abbildung 3):

LS1 (gelöscht, betrifft die interne logische Schnittstelle zwischen Netzkonnektor und Anwendungskonnektor)

LS2 Eine Schnittstelle zu den Clientsystemen, die physisch über das LAN (PS1) des Leistungserbringers erreichbar sind.

LS3 Eine Schnittstelle zu den Fachmodulen NFDM, AMTS und ePA (alle nicht Teil des EVG). Da diese Kommunikation jedenfalls innerhalb des Konnektors erfolgt, wird hier keine physische Schnittstelle zugeordnet.

LS4 Eine Schnittstelle zum VPN Konzentrator der zentralen TI-Plattform (WAN, via PS2[10]).

[10] In der Konnektorspezifikation [**Fehler! Textmarke nicht definiert.**] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

LS5 Eine Schnittstelle zum VPN Konzentrator des sicheren Zugangspunkt des Internet-Providers (SIS) (WAN, via PS2[11]).

LS6 Eine Schnittstelle zu Fachdiensten, die mittels eines VPN über das Transportnetz (WAN, via PS2[12]) erreicht werden.

LS7 Eine Schnittstelle zu PKI- und anderen Diensten (WAN, via PS2[13]). Dazu zählen der TSL-Dienst, der CRL-Download, sowie der OCSP-Dienst.

LS8 Eine Schnittstelle zum Konfigurationsdienst (WAN, via PS2[14]).

LS9 Eine Schnittstelle zu eHealth-Kartenterminals (LAN, via PS1).

LS10 Eine Schnittstelle zu Chipkarten außerhalb des EVG, die über eHealth-Kartenterminals angesprochen werden (LAN, via PS1).

LS11 *entfallen*.

LS12 Eine Schnittstelle zu einem Sicherheitsmodul (gSMC-K, via PS3). Aufgrund der Annahme A.AK.gSMC-K werden keine Angriffe über diese Schnittstelle betrachtet.

LS13 Eine Schnittstelle zur lokalen Managementfunktionen des Netzkonnektors (via PS1).

LS14 Eine Schnittstelle zur Signaleinrichtung (Signalisierung) zur Statusanzeige. Über diese Schnittstelle werden die LEDs zur Anzeige des Verbindungsstatus und zur Anzeige von Fehlerzuständen (kritische Betriebszustände) gemäß Konnektor-Spezifikation [92], Abschnitt 3.3 (via PS4) angesteuert.

LS15 Eine Schnittstelle zur Vertrauenswürdigen Ausführungsumgebung (VAU) des ePA-Aktensystems die mittels eines VPN über das Transportnetz (WAN, via PS2[15]) und unter Verwendung der LS4 erreicht wird.

LS16 Eine Schnittstelle zum Schlüsselgenerierungsdienst SGD (SGD-HSM) die mittels eines VPN über das Transportnetz (WAN, via PS2[16]) und unter Verwendung der LS4 erreicht wird.

[11] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[12] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[13] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[14] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[15] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[16] In der Konnektorspezifikation [Fehler! Textmarke nicht definiert.] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

Hinweis: Die Kommunikation mit SGD1 und SGD2 wird als eine logische Schnitstelle (LS16) betrachtet. Die Kommunikation mit dem ePA Aktensystem unter Verwendung der VAU (LS15) umfasst die Kommunikation mit der Autorisierungskomponente und der Dokumentenverwaltung.

Hinweis: Im Fall der Vergabe von ad-hoc Berechtigungen durch den Versicherten für den Zugriff auf die Daten der ePA erfolgt eine Kommunikation des Konnektors mit dem Zugangsgateway des Versicherten. Diese Kommuikation wird als Zugriff auf einen Fachdienst verstanden und ist in LS6 enthalten.

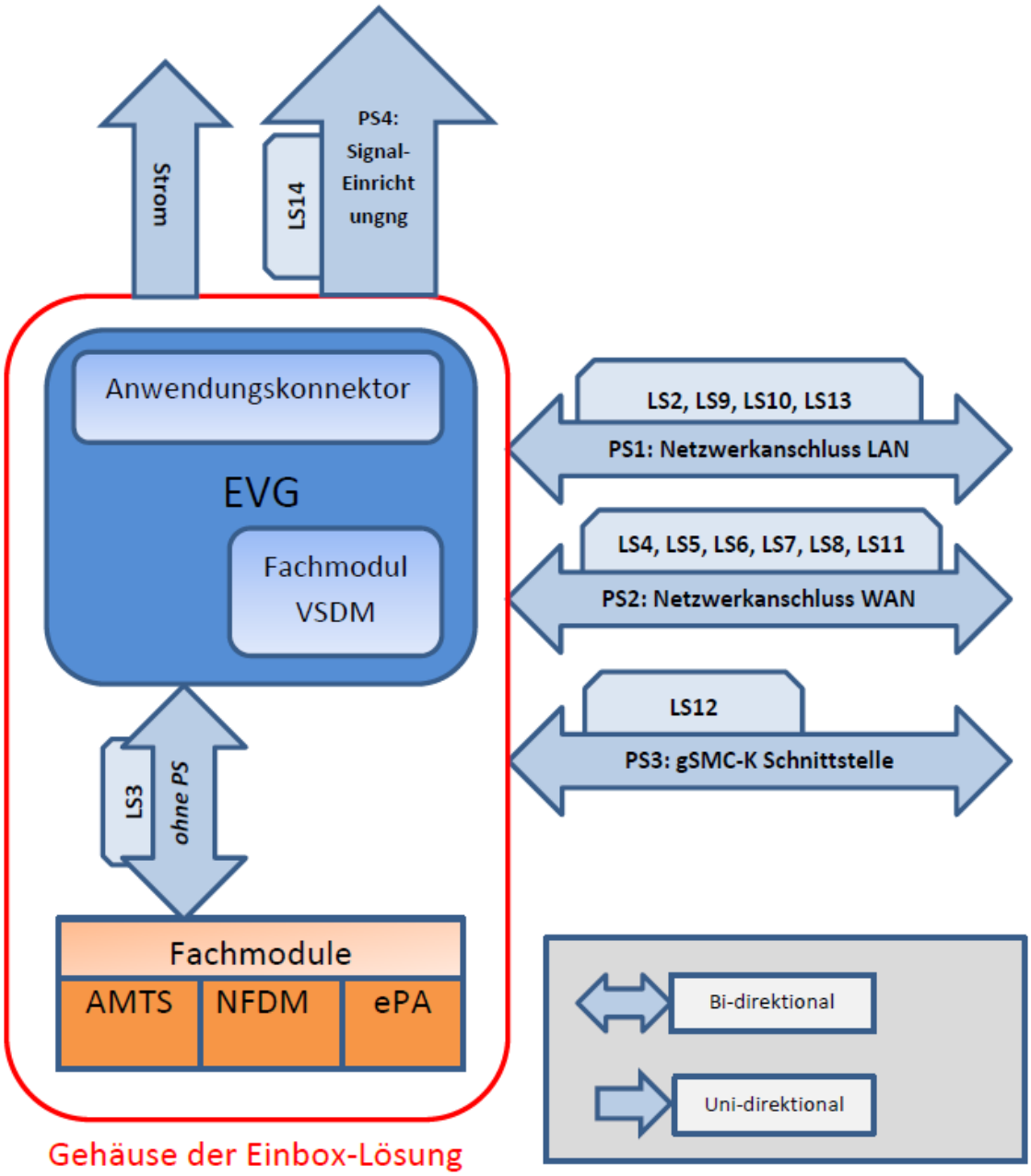


Abbildung 5: physische und logische externe Schnittstellen des Konnektors

1.3.4. Aufbau und physische Abgrenzung des Netzkonnektors

Zur Gesamtarchitektur und für einen Überblick über die Kernkonzepte sei auf die Konnektor-Spezifikation [92] verwiesen.

Anwendungshinweis 7: Die Abbildung 6 stellt das allgemeine Architekturkonzept des gesamten Konnektors dar. Hieraus wird die Einordnung des EVG ersichtlich.

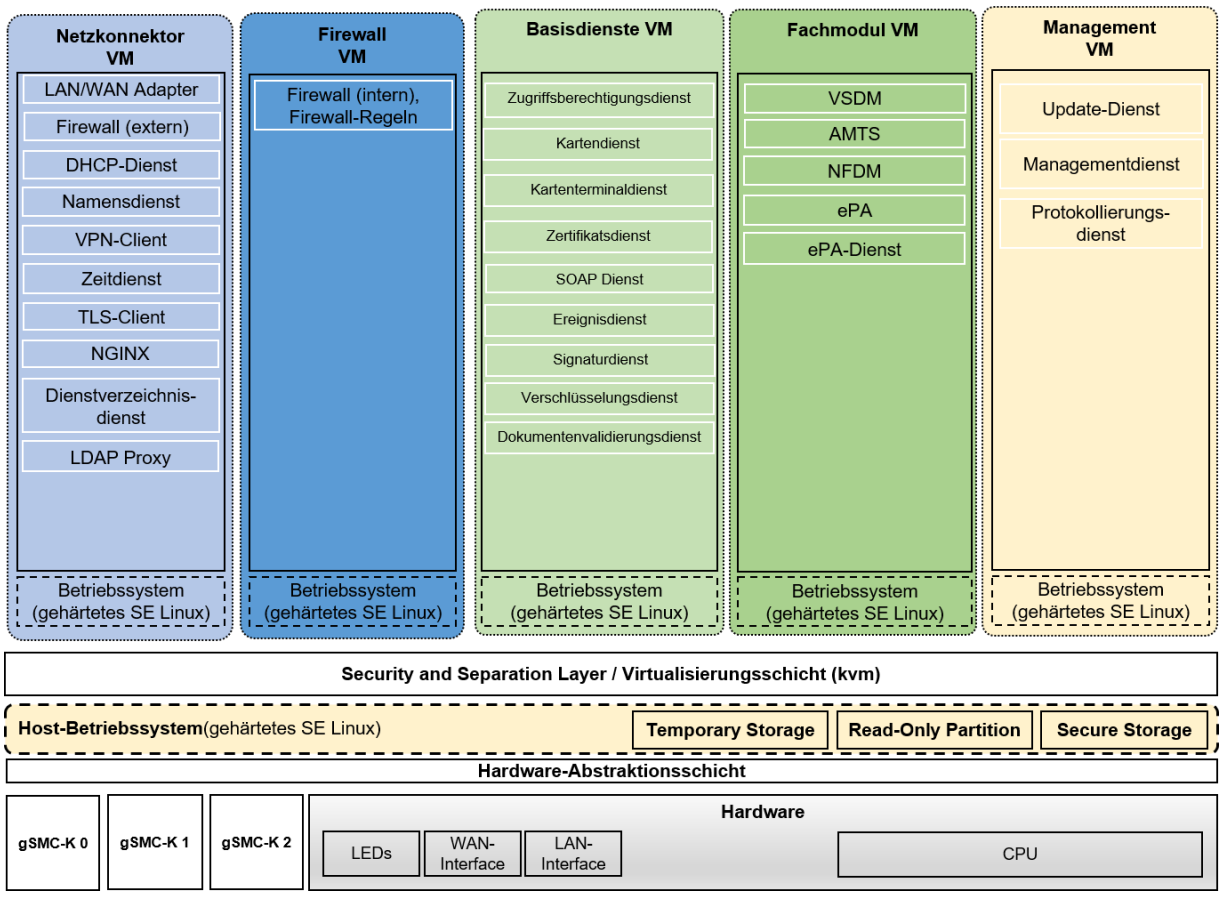


Abbildung 6: Konnektor Architekturkonzept (schematisch)

Architekturübersicht

Der in diesem Security Target definierte Evaluierungsgegenstand umfasst die Software des Konnektors und die Betriebsdokumentation. Die Hardware des Konnektors ist nicht Teil des EVGs; diese ist in Kapitel 1.3.6 genauer beschrieben. In Abbildung 6 wird die gesamte Architektur des Konnektors inklusive Hardware und Softwareanteile des Anwendungskonnektors dargestellt.

Die Software für den Betrieb eines Konnektors wird modular aufgebaut, wobei jedem Modul eine dezidierte Aufgabe übertragen wird und dieses jeweils unabhängig und unbeeinflusst von anderen Modulen betrieben wird.

Als Grundlage für die Umsetzung des Konnektors wird ein gehärtetes Linux-System eingesetzt, welches als Betriebssystem unter anderem für die Verwaltung der Hardwareressourcen (z.B. CPU Scheduling, Arbeitsspeicherverwaltung) verantwortlich zeichnet. Das Linux-System wurde genau an die Sicherheits- und Anwendungsanforderungen des Konnektors angepasst.

Der HAL (Hardware Abstraction Layer) ist integraler Bestandteil des Kernels und wird mit Hilfe von Linux Gerätetreibern umgesetzt; beispielsweise kommt für die Kommunikation mit der gSMC-K ein entsprechender Linux-Treiber zum Einsatz. Damit ist es Anwendungen möglich, mit einer Gerätekarte mittels APDUs (Application Protocol Data Unit) auf sicherem Wege zu kommunizieren.

Aufbauend auf dem HAL und dem Betriebssystem werden einzelne Module – wie beispielsweise Fachmodule oder das Management-Modul – primär mittels Java und C/C++ implementiert und jeweils in eigenständigen Anwendungscontainern betrieben. Die Module sind in entsprechend ihrer Funktionalität gruppiert und in verschiedene virtuelle Umgebungen eingebunden. Somit sind nicht nur die betriebenen Module, sondern auch die gemeinsamen Betriebssystem-Komponenten logisch separiert. Dazu wird ein Virtualisierungs-Hypervisor eingesetzt welcher als Teil des Linux-Host-Betriebssystems installiert und betrieben wird.

Im Folgenden werden die einzelnen Funktionsblöcke des Konnektors beschrieben, in denen als virtuelle Umgebungen (Virtual Machine, VM) einzelne Module zusammengefasst sind:

(1) **Netzkonnektor VM:** Diese VM übernimmt die Aufgabe der Sicherung von Netzwerkkommunikation im lokalen Netzwerk (z.B. Kommunikation mit angeschlossenen Kartenterminals) sowie mit der TI-Plattform. Dies umfasst beispielsweise Implementierung von lokalen Netzwerkdiensten (z.B. DNS), Firewall und die TLS und VPN-Anbindung an die TI-Plattform, für welche auch Routing-Funktionalität bereitgestellt wird und somit die Transportsicherung der TI-Plattform sichergestellt wird.

(2) **Firewall VM:** Diese VM überwacht die Kommunikation der einzelnen Module untereinander. Dabei handelt es sich nicht um die nach außen angebotene Firewall-Funktionalität des Netzkonnektors. Diese wird in der Netzkonnektor VM implementiert. Die Firewall VM als zentraler Dienst übernimmt auch Protokollierungsaufgaben.

(3) **Basisdienste VM:** Die Basisdienste VM setzt die Funktionalität des Anwendungskonnektors um. Der Basiskonnektor übernimmt auch die Aufgabe der Kommunikation mit den Gerätekarten (über den Treiber), und ist die einzige VM, die über die Treiber-API auf die Gerätekarten zugreifen darf. Sicherheitsaufgaben wie Verschlüsselung oder Signaturerstellung bzw. -prüfung sind ebenfalls durch den Basiskonnektor abgebildet.

(4) **Fachmodule VM:** Durch die beschriebene Architektur wird ein flexibler Einsatz von mehreren unterschiedlichen Fachmodulen ermöglicht. Solche können im Rahmen eines Firmware-Updates über das „Management-Modul“ installiert und verwaltet werden.

(5) **Management VM:** Implementiert das Management-Interface für lokale Administration. Damit wird einem Benutzer die Möglichkeit zur Verwaltung des Konnektors gegeben. Unter anderem wird durch diese VM die Zertifikats- und Userverwaltung abgebildet.

Diese VM übernimmt auch die Aufgabe, alle anderen Module über vorgesehene Schnittstellen zu konfigurieren, sodass sämtliche Systemparameter (inkl. anderer Module, Betriebssystem) in dieser VM abgebildet werden können. Damit wird eine einzelne und zentrale Stelle zur Systemkonfiguration des Konnektors geschaffen.

Zusätzlich kann ein autorisierter Benutzer über das Management-Interface Informationen zum Systemstatus (z.B. Betriebsstatus der einzelnen Module) abrufen. Des Weiteren wird der Firmware-Upgrade Prozess in dieser VM abgebildet. Eine neue

Firmware-Version kann nur nach bestandener Integritäts- und Authentizitätsprüfung sowie bestandener Versionsprüfungen installiert werden.

Ausschließlich die Management VM hat die Möglichkeit signierte Firmware-Updates einzuspielen.

Alle in Tabelle 1 benannten Komponenten des Konnektors befinden sich innerhalb eines Gehäuses. Die physische Abgrenzung des Netzkonnektors ist durch die „Einbox-Lösung“ des Konnektors definiert.

1.3.5. Logische Abgrenzung: Vom EVG erbrachte Sicherheitsdienste

Die im Folgenden beschriebene Sicherheitsfunktionalität stellt die Mindestanforderung an den EVG dar, d.h. ein Konnektor, der dieses Schutzprofil erfüllt, muss mindestens diese Anforderungen erfüllen.

1.3.5.1. Logische Abgrenzung: Vom Netzkonnektor erbrachte Sicherheitsdienste

Der Netzkonnektor erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [92] definierten Schnittstellen weitgehend automatisch. Der Netzkonnektor ermöglicht ein Management (Administration) nach Autorisierung des Administrators. Die Autorisierung des Administrators erfolgt sowohl für den Netzkonnektor als auch für den Anwendungskonnektor durch das Management Modul (siehe Abschnitt 1.3.4, Management VM). Dieses Modul wird in diesem Security Target dem Netzkonnektor zugeordnet. Die Authentisierung des Administrators erfolgt daher durch den Netzkonnektor selbst.

Anwendungshinweis 8: Authentisierung des Administrators: Das Mangement Modul implementiert einen gemeinsamen Administrator-Account für Netzkonnektor und Anwendungskonnektor. Die Authentisierung des Konnektor-Administrators wird formal dem NK zugeordnet. Der Anwendungskonnektor (AK) übernimmt den Authentisierungszustand. Aufgrund der Annahme A.AK.phys_Schutz ist dabei keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) erforderlich. Da der Netzkonnektor die Authentisierung des Administrators selbst durchführt; wurde das Umgebungsziel OE.NK.Admin_Auth aus dem PP [77] in ein EVG-Ziel O.NK.Admin_Auth umgewandelt.

Anwendungshinweis 9: Vollständigkeit der Dienste: Die Dienste wurden aus dem Netzkonnektor PP [77] übernommen. Es wurden keine zusätzlichen Dienste modelliert.

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

Der Netzkonnektor erbringt die folgenden Sicherheitsdienste gemäß PP BSI-CC-PP-0097-V2:

VPN-Client: Der Netzkonnektor 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 Netzkonnektor einen sicheren Kanal (VPN) zum SIS her. Dieser Kanal dient der

Verbindung der lokalen Netzwerke der Leistungserbringer mit dem Internet. Der Netzkonnektor 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.
Die Nutzdaten, die über das VPN übertragen werden, werden hinsichtlich ihrer Vertraulichkeit und Datenintegrität geschützt (Verschlüsselung und Integritätsschutz der Daten vor dem Versenden bzw. der Entschlüsselung und der Integritätsprüfung nach dem Empfangen). Dazu wird für die VPN-Verbindung ein Sitzungsschlüssel vereinbart.
Der Netzkonnektor muss die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen erzwingen und ungeschützten Zugriff auf das Transportnetz verbieten. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[17], aber er muss ihre versehentliche Preisgabe verhindern.

Dynamischer Paketfilter: Der Netzkonnektor bindet die Clientsysteme sicher an die Telematikinfrastruktur, den SIS und die Bestandsnetze (über die TI) an. Dazu verfügt der Netzkonnektor über die Funktionalität eines dynamischen Paketfilters, welcher entsprechende Regeln umsetzen kann. Der Netzkonnektor 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 Netzkonnektor beschränkt den freien Zugang zu dem und von dem als unsicher angesehenen Transportnetz. Die Inhalte der Kommunikation zur Telematikinfrastruktur werden von Netzkonnektor nicht ausgewertet. In jedem Fall unterbindet der Netzkonnektor direkte Kommunikation (außerhalb von VPN-Kanälen) ins Transportnetz (WAN, Internet) mit Ausnahme der für den VPN-Verbindungsaufbau erforderlichen Kommunikation[18] sowie Verbindungen zum CRL Download Server.

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

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

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

Anwendungshinweis 12: Der Netzkonnektor enthält kein Application Layer Gateway in dem Sinne, dass der Anwendungskonnektor auf einem eigenen Layer implementiert wird. Vielmehr ist der Gesamtkonnektor modular aufgebaut. Die einzelnen Module laufen auf einem Security and Separation Layer (Virtualisierungsschicht), siehe auch Abschnitt 1.3.4. Aus Sicht des Gesamtkonnektors wird zudem der Anwendungskonnektor topologisch von beiden Seiten von einem Paketfilter umgeben (LAN-seitig und WAN-seitig, d.h. gegenüber dem Clientsystemnetz und gegenüber dem Transportnetz; siehe auch Einsatzumgebung).

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

Anwendungshinweis 13: Die Entscheidung, für welche Verbindungen diese TLS-Kanäle genutzt werden, liegt beim Anwendungskonnektor, also außerhalb des Netzkonnektors.

Der Netzkonnektor 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 Netzkonnektor kann die synchronisierte Zeit anderen Komponenten des Konnektors zur Verfügung stellen. Die vom Netzkonnektor bereitgestellte Zeit-Information wird für die Prüfung der Gültigkeit von Zertifikaten genutzt, und um die Audit-Daten des Sicherheits-Logs mit einem Zeitstempel zu versehen.

Anwendungshinweis 14: Durch den Netzkonnektor erfolgt eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK. Die Konnektor-Spezifikation [92] sieht vor, dass die Zeitsynchronisation ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform erfolgt, d.h. über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur.

DHCP-Dienst: Der Netzkonnektor stellt an der LAN-Schnittstelle (PS1) die Funktion eines DHCP Servers gemäß RFC 2131 [46] und RFC 2132 [47] zur Verfügung.

DNS-Dienst: Der Netzkonnektor stellt an der LAN-Schnittstelle (PS1) und für den AK die Funktion eines DNS-Servers zur Verfügung.

Gültigkeitsprüfung von Zertifikaten: Der Netzkonnektor muss die Gültigkeit der Zertifikate des Kommunikationspartners überprüfen, die für den Aufbau eines VPN-Kanals oder TLS-Kanals verwendet werden.[19] Zu diesem Zweck wird eine TSL (Trust-Service Status List) verteilt, welche Zertifikate von Diensteanbietern enthält, die Gerätezertifikate ausstellen können. Der Netzkonnektor kann anhand der aktuell gültigen TSL die Gültigkeit der Gerätezertifikate seiner Kommunikationspartner prüfen. Ferner wird eine zugehörige CRL (Certificate Revocation List)

[19] 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.

bereitgestellt, die der Netzkonnektor ebenfalls auswertet. Außerdem überprüft der Netzkonnektor, dass die verwendeten Algorithmen gültig sind. Siehe auch Sicherheitsdienst VPN-Client.

Anwendungshinweis 15: Die Prüfung der Algorithmen erfolgt implizit durch den Netzkonnektor, indem sichergestellt wird (im Rahmen der Evaluierung), dass der Netzkonnektor nur gültige Algorithmen verwendet. Die Verwendung ungültig gewordener Algorithmen wird dadurch verhindert wird, dass – unter Verwendung des Software-Update-Mechanismus des Konnektors – ein Update eingespielt wird.

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

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

Darüber hinaus implementiert der Netzkonnektor folgende übergeordnete Dienste:

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

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

Selbsttests: Der Netzkonnektor bietet seinen Benutzern eine Möglichkeit, die Integrität des Netzkonnektors zu überprüfen.

Protokollierung: Der Netzkonnektor führt ein Sicherheits-Log (security log) in einem nicht-flüchtigen Speicher, so dass es auch nach einem Neustart zur Verfügung steht. Der für das Sicherheits-Log reservierte Speicher muss hinreichend groß dimensioniert sein. Die zu protokollierenden Ereignisse orientieren sich an der Konnektor-Spezifikation [92].

Anwendungshinweis 17: Die Auswertung des Sicherheits-Logs erfolgt durch die Einsatzumgebung. Es werden vom Netzkonnektor keine Auswertungen durchgeführt, die über die Anforderungen der Konnektor-Spezifikation [92] hinausgehen.

Anwendungshinweis 18: Die geschützte Speicherung des Protokolls (u. a. zyklisches Überschreiben, Schutz gegen Manipulation durch den Administrator) wird als übergreifende Funktionalität im PP [78] gefordert (siehe dort, FAU_STG.1/AK und FAU_STG.4/AK).

Administration: Der Netzkonnektor bietet eine lokale Managementschnittstelle an. Die Managementschnittstelle wird durch das Management Modul vom Netzkonnektor umgesetzt.

Anwendungshinweis 19: An der Managementschnittstelle werden Wartungsaktivitäten durchgeführt, wie die Verwaltung von Clientsystemen, Verwaltung von LAN/WAN Anbindungen inkl. Einstellungen bzgl. VPN, Konfiguration von Diensten (Kartendienst, Zertifikatsdienst, Kartenterminaldienst, Systeminformationsdienst, Protokollierungsdienst, Zeitdienst, Signaturdienst) und Fachmodulen (VSDM), Einstellungen bezüglich DHCP und DNS, Management des Informationsmodells und des allgemeinen Betriebes, Konfiguration zum KSR Client. Verwaltung von Registrierungsinformationen und Benutzerverwaltung.
Eine Möglichkeit zur Fernwartung (remote Management) ist nicht implementiert.

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

1.3.5.2. Vom Anwendungskonnektor erbrachte Sicherheitsdienste

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

Signaturdienst: Der EVG ermöglicht im Sinne der eIDAS-VO [8] 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 (HBAx[20]) mit QES-Signaturschlüsseln zum Einsatz. Für die Erzeugung der nonQES-Signatur wird ein HBAx oder die SM-B[21] mit non-QES-Signaturschlüsseln verwendet.

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.

Sie enthält:

- Signaturart: „qualifizierte elektronische Signatur“, „nicht-qualifizierte elektronische Signatur“,
- Format der zu signierenden Daten: XML-Dokument, Adobe Portable Document Format, Text-Dokument, TIFF-Dokument, Binärstring,
- Signaturtyp der signierten Daten,

[20] HBAx schließt für den Signaturdienst den HBA und die Vorläuferkarten HBA-qSig und ZOD-2.0 ein.

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

- Signaturattribute: einfache Dokumentensignatur, Parallelsignatur, Gegensignatur.

Die Signaturart qualifizierte elektronische Signatur wird durch die eIDAS-VO [8] definiert. Alle anderen, diesen Anforderungen an qualifizierte elektronische Signaturen nicht genügenden durch den Signaturdienst erzeugte Signaturen sind nicht-qualifizierte elektronische Signaturen. Nach dem Format der zu signierenden Daten werden Binärstring und Dokumente unterschieden.
Ein Binärstring besteht aus maximal 512 Bit, über den unabhängig von der internen Struktur eine digitale Signatur (non-QES gemäß PKCS#1v2.2, [31]) mit Authentisierungsschlüsseln eines HBAx oder einer SM-B berechnet wird.
Dokumente werden als zu signierende oder zu prüfende Dateien übergeben. Laut Spezifikation Konnektor [92] werden folgende Dokumenten-Formate zur Signaturerstellung und Signaturprüfung unterstützt[22]:

- XML-Dokumente,
- Adobe Portable Document Format (PDF/A),
- Text-Dokumente,
- TIFF-Dokumente,
- Binärdokumente (nur nichtqualifizierte (non-QES) elektronische Signaturen).

Folgende Signaturtypen werden abhängig von dem Format der zu signierenden Dokumente und von konfigurierten Parametern unterstützt (vergl. [92], Kap. 4.1.8):

- Adobe-Standard (für PDF/A-Dokumente): PAdES
- CMS (RFC 5652, [34]): CAdES
- XMLDSig (für XML-Dokumente): XAdES
- S/MIME [35]
- Signaturvarianten: enveloped signature, enveloping signature, detached signature.

Für XML-Dokumente und XML-Signaturen umfasst die Signaturrichtlinie

- XML-Schemadefinition (XSD): beschreibt die Struktur der zu signierenden Daten,

Das konkret auszuwählende Format ist in Kapitel 4.1.8 von [92] festgelegt.

Ein beispielhafter Ablauf einer qualifizierten Signatur-Erzeugung im Fall der fehlerfreien Ausführung ist in BSI-CC-PP-0098-V3, Abschnitt 1.3.5.2, zu finden.

Anwendungshinweis 20: Die genauen Abläufe der Signaturerstellung und Prüfung sind der Spezifikation Konnektor [92] und den dort referenzierten Dokumenten zu entnehmen.

Anwendungshinweis 21: Weitere Informationen zu den Abläufen sind der Spezifikation Konnektor [92] und den dort referenzierten Dokumenten zu entnehmen.

[22] Die entsprechenden Standards sind der Konnektor-Spezifikation zu entnehmen, siehe Tabelle 148 in [**Fehler! Textmarke nicht definiert.**]

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 [92] 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 BSI TR-03116-1 [76] 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, [34]) an. Darüber hinaus werden folgende formaterhaltende Ver-/Entschlüsselungsmaßnahmen unterstützt:

- Hybride Ver-/Entschlüsselung von XML Dokumenten nach [21],
- Hybride Ver-/Entschlüsselung von MIME-Dokumenten nach SMIME Standard (RFC 5751, [35]).

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.

Zusätzlich bietet der sichere Datenspeicher einen separaten Bereich, der nur für Administratoren lesbar und schreibbar ist. Die Absicherung dieses Bereiches erfolgt durch kryptographische Mechanismen.

Gesicherte Kommunikation: Die Absicherung der Kommunikation über die externen Netzwerk-Schnittstellen erfolgt auf niedriger Netzwerk-Schicht (Layer 3: IP) 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[23]. 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.
- Verbindungen zwischen dem EVG und dem TSL-Dienst für den Download der Hash-Datei TSL(ECC-RSA)
- Verbindung zwischen dem EVG und dem SGD-RVE
- Verbindung zwischen dem EVG und der ePA Aktensystem
- Verbindung zwischen dem EVG und dem Zugangsgateway des Versicherten im Fall von ad-hoc Berechtigungen

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: 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[24]. 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-

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

[24] Siehe auch Sicherheitsdienst „gesicherte Kommunikation“

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.

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 [75]. 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 [92], 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.

LDAP-Proxy: Der LDAP-Proxy ermöglicht Fachmodulen und Clientsystemen die Nutzung des zentralen Verzeichnisdienstes der TI mittels des Lightweight Directory Access Protocol.

1.3.6. Non-EVG hardware/software/firmware

Der EVG umfasst die Software des Netzkonnektors, des Anwendungskonnektors und das Fachmodul VDSM. Dabei wird der Netzkonnektor immer mit den Konnektorteilen Anwendungskonnektor und der Security Module Card Konnektor gSMC-K gemeinsam betrieben, siehe auch die Beschreibung zur Einsatzumgebung in Kapitel 1.3.2.

Der Netzkonnektor bietet dabei dem Anwendungskonnektor eine sichere Plattform und stellt die in diesem Security Target definierten Sicherheitsfunktionen zur Verfügung. Dazu nutzt der EVG die Sicherheitsfunktion der gSMC-K. Das Betriebssystem und das Objektsystem der gSMC-K sind von der gematik zugelassen.

Anwendungshinweis 22: Der Konnektor wird als reine Software-Lösung implementiert. Die Hardware ist nicht Teil des EVGs.

Die Hardware des Einbox-Konnektors ist in einem vollständig geschlossenen Gehäuse mit externem Netzteil. Das Gehäuse besitzt die in Kapitel 1.3.3.1 beschriebenen physischen Schnittstellen, insbesondere Netzwerkports für WAN und LAN Verbindungen, USB-Ports und LEDs für die Signaleinrichtung. Im Gehäuse sind drei gSMC-Ks des Konnektors verbaut. Als gSMC-Ks werden durch die gematik zugelassene STARCOS 3.6 Health SMCK R1 verwendet. 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 LAN und WAN
Smartcard-Leser (für gSMC-K)	3x interne CCID kompatible USB Leser oder Onboard-Kartenleser für ID-000 Karten (SIM- Kartenformat)
RTC	Real-Time-Clock mit einem definierten Drift von maximal +/- 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:

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

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

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

und unter Berücksichtigung von

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

Es wurden funktionale Sicherheitsanforderungen (FPT_EMS.1, siehe Abschnitt 5.1, und FIA_API.1/AK, siehe Abschnitt 5.2) definiert, die nicht in CC Teil 2 [2] enthalten sind. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [3] entnommen.

Daher ist dieses Security Target:

CC Teil 2 [2] erweitert (extended) und

CC Teil 3 [3] konform (conformant).

2.2. Security Target-Konformität

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

> Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3, Version 1.5.9 vom 15.04.2021, Bundesamt für Sicherheit in der Informationstechnik (BSI), [78].[25]

[25] Vorgreifend wird dieses Schutzprofil im vorliegenden Dokument mit der voraussichtlichen PP-Registrierung BSI-CC-PP-0098-V3 geführt.

2.3. Paket-Konformität

Das Schutzprofil fordert 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).

In diesem Security Target werden die vom Schutzprofil BSI-CC-PP-0098-V3 geforderten Vertrauenswürdigkeitsanforderungen übernommen, und es wurden keine Komponenten hinzugefügt, die über das BSI-CC-PP-0098-V3 hinausgehen.

2.4. Begründung der Konformität

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

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

Das Security Target übernimmt die Definition des EVG-Typs sowie des Sicherheitsproblems, der Sicherheitsziele und der Sicherheitsanforderungen aus dem zugrundeliegenden Protection Profile BSI-CC-PP-0098-V3. Da das Security Target keine Konformität zu weiteren Schutzprofilen behauptet, können auch keine Widersprüche zwischen diesem Security Target und weiteren Schutzprofilen im EVG-Typ oder in der Definition des Sicherheitsproblems, der Sicherheitsziele oder der Sicherheitsanforderungen auftreten.

Das zugrundeliegende Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, wie sie in CC Teil 3 [3] definiert ist, zusammen mit der Komponente AVA_VAN.3, um Schutz gegen “enhanced basic” Angriffspotenzial zu erreichen. Durch direkte und indirekte Abhängigkeiten der Komponente AVA_VAN.3 müssen die Komponenten ADV_IMP.1 und ALC_TAT.1 neu aufgenommen werden und die Komponenten ADV_TDS.3 und ADV_FSP.4 augmentiert werden. Darüber hinaus wurde die Stufe EAL3 noch um die Komponente ALC_FLR.2 augmentiert, die keine Abhängigkeiten besitzt; für die Gründe dazu siehe Abschnitt 6.5.9. Das Security Target übernimmt die Vertrauenswürdigkeitsstufe des Schutzprofils. Damit sind alle Anforderungen an die Konformität erfüllt.

3. Definition des Sicherheitsproblems

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

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

3.1.1.1. Durch den Netzkonnektor zu schützende Werte

Die in diesem Abschnitt genannten zu schützenden Werte sind dem Schutzprofil BSI-CC-PP-0097-V2 [77] entnommen.

Der Begriff „zu schützende Daten der TI und der Bestandsnetze“ bezeichnet im Folgenden stets medizinische oder sonstige personenbezogene Daten (einschließlich Daten des Versicherten), die aus dem Zuständigkeitsbereich des Leistungserbringers in die Verantwortung der Telematikinfrastruktur bzw. in die Bestandsnetze übergehen, und umgekehrt. Diese Daten sind *User Data* im Sinne der Common Criteria. Sie umfassen bei den Pflichtanwendungen nach § 291 a SGB V [10] mindestens die Versichertenstammdaten[26] und elektronische Verordnungen (eVerordnungen) sowie sonstige Daten, die im Rahmen der Abwicklung dieser Pflichtanwendungen entstehen (etwa Dispensierdaten).

Primäre Werte

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 während der Übertragung zwischen Konnektor und	Vertraulichkeit, Integrität, Authentizität	Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform werden zu schützende Daten der TI und der Bestandsnetze ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch

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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zentraler Telematikinfra-struktur-Plattform (beide Übertragungs-richtungen)		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.Zert_Prüf, 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.AK.phys_Schutz
in der zentralen Telematikinfrastruktur-Plattform oder auf Chip-karten 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.AK.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. 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

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

Tabelle 3: Primäre Werte

Die primären Werte, deren zu schützenden Eigenschaften und das daraus abgeleitete Bedrohungspotential bzw. erforderliche Annahmen entsprechen Tabelle 1 des zugrundeliegenden PPs [77]

Sekundäre Werte

Die sekundären Werte sind in der folgenden Tabelle 4 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze im EVG	Vertraulichkeit, Integrität	Auch während der Verarbeitung im EVG müssen zu schützende Daten der TI und der Bestandsnetze gegen unbefugte Kenntnisnahme und Veränderung geschützt werden. ⇒ T.NK.local_EVG_LAN T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN
kryptographisches Schlüsselmaterial (während seiner Speicherung im EVG oder Verwendung durch den EVG)	Vertraulichkeit, Integrität, Authentizität	Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der EVG seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikationspartners sicherzustellen. ⇒ A.AK.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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
Authentisierungs-geheimnisse (im EVG gespeicherte Referenzdaten und zum EVG übertragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungsgeheimnissen (z. B. Passwort für Administratorauthentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.AK.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 der EVG seine Sicherheitsleistungen korrekt erbringt. ⇒ A.AK.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.AK.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_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit
Systemzeit	Verfügbarkeit, Gültigkeit	Der EVG muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern synchronisieren. Die Zeit wird für die Prüfung der Gültigkeit von VPN-Zertifikaten sowie für die Erzeugung von Zeitstempeln in Sicherheits-Log-Daten oder Audit-Daten verwendet. ⇒ T.NK.TimeSync

Tabelle 4: Sekundäre Werte

Die sekundären Werte, deren zu schützenden Eigenschaften und das daraus abgeleitete Bedrohungspotential bzw. erforderliche Annahmen entsprechen Tabelle 2 des zugrundeliegenden PPs [77].

3.1.1.2. Durch den Anwendungskonnektor zu schützende Werte

Über die in Abschnitt 3.1.1.1 aufgeführten Werte hinaus werden für den Konnektor weitere zu schützende Werte identifiziert, die in Tabelle 5 zusammengestellt sind.

Die zu schützenden Werte sind in den folgenden Tabellen Tabelle 5 und Tabelle 6 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	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 nicht unautorisiert verändert oder eingesehen werden.[27] ⇒ T.AK.Mani.EVG, T.AK.Mani.TI, A.AK.Konnektor, A.AK.phys_Schutz

Tabelle 5: primäre Werte des Anwendungskonnektors

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

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
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
Managementdaten 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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Authentisierungs-geheimnisse bei der Speicherung und Bearbeitung im EVG	Integrität, Vertraulichkeit	Die Vertraulichkeit und Integrität von Authentisierungs-geheimnissen (z. B. Passwort für 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

Der für die Signaturerstellung notwendige Signaturschlüssel (SCD[28]) ebenso wie die Authentisierungsreferenzdaten (SRAD[29]) 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 in diesem Abschnitt genannten Entitäten sind dem Schutzprofil BSI-CC-PP-0097-V2 [77] entnommen.

In der Einsatzumgebung des Netzkonnektors gibt es folgende externe Einheiten:

AK Anwendungskonnektor,

VPN-TI entfernter VPN-Konzentrator, der den Zugriff auf die Telematikinfrastruktur vermittelt,

[28] Englisch: signature-creation data

[29] Englisch: signatory reference authentication data

VPN-SIS entfernter VPN-Konzentrator, der den sicheren Zugriff auf das Internet realisiert,

DNS-ext (externer) DNS-Server für den Namensraum Internet

Zeit-ext (externer) Zeit-Server des Zugangsnetzproviders

CS Clientsystem,

TSL/CRL Bereitstellungspunkte für TSL und CRL

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

Angreifer ein Angreifer.

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

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

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

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

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 in diesem Abschnitt genannten Entitäten sind dem Schutzprofil BSI-CC-PP-0097-V2 [77] entnommen.

Es werden die folgenden Objekte betrachtet:

CS-Daten lokal beim Leistungserbringer (in Clientsystemen im LAN) gespeicherte zu schützende Daten der TI und der Bestandsnetze,

VPN-Daten-TI zu schützende Daten der TI und der Bestandsnetze während des Transports zwischen NK und VPN-K der Telematikinfrastruktur,

VPN-Daten-SIS *zu schützende Nutzerdaten* während des Transports zwischen NK und VPN-SIS

TI-Daten entfernt in den Datenbanken der Telematikinfrastruktur bzw. den Bestandsnetzen gespeicherte zu schützende Daten der TI und der Bestandsnetze.

Es wird davon ausgegangen, dass die VPN-Daten durch den zwischen NK und VPN-Konzentratoren implementierten sicheren Kanal (d.h. durch das VPN) geschützt werden und dass die TI-Daten nur in verschlüsselter Form gespeichert vorliegen (z. B. eVerordnung) (siehe A.AK.sichere_TI in Abschnitt 3.4.1). Die Sicherheit der **Clientsystem**e 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 [1], 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 Managementschnittstelle (vergl. [92], 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 Leistungserbringer sind spezielle Clientsysteme und umfassen die Praxisverwaltungssysteme für Ärzte, Zahnärzte und Psychotherapeuten, die Krankenhausinformationssysteme der Krankenhäuser und die Apotheken-verwaltungssysteme der Apotheker und stellen die Anwendungsprogramme für die	Bei Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: Öffentlicher Schlüssel Ohne Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: keine Sicherheitsattribute

Benutzer des Anwendungskonnektors	**Beschreibung**	**Sicherheitsattribut**
	Leistungserbringer und Versicherten zur Verfügung. Ohne Nutzung eines TLS-Kanals kann der EVG nicht zwischen einer beliebigen Komponente im LAN und einem Clientsystem unterscheiden.	
Fachmodul	Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen 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 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 Client-systems	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.	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.
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. [94] Kap. 3.7).	Identität: Umfasst die - ID.SMKT.AUT der gSMC-KT des eHealth-Kartenterminals, - physische Adresse im LAN-LE. Authentisierungsreferenzdaten: Authentisierungsreferenzdaten zur

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
		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[30] als gSMC-KT. - C.SMC.AUTD_RPS_CVC[31] mit CHAT als PIN-Sender.
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[32].	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

[30] C.SMKT.AUT steht hier für C.SMKT.AUT.R2048 und den optionalen C.SMKT.AUT.R3072 der Spezifikation des Objektsystems der gSMC-KT [102].

[31] C.SMC.AUTD_RPS_CVC steht hier für C.SMC.AUTD_RPS_CVC.R2048, C.SMC.AUTD_RPS_CVC.E256 und den optionalen C.SMC.AUTD_RPS_CVC.E384 der Spezifikation des Objektsystems der gSMC-KT [102].

[32] Beispiel für die Interaktion EVG/Benutzer über die eHealth-Kartenterminals ist die lokale oder entfernte PIN-Eingabe. Das Lesen von Versichertenstammdaten erfolgt unter Steuerung der Einsatzumgebung (z. B. des Clientsystems), die durch den EVG nur kontrolliert, aber nicht gesteuert wird.

Benutzer des Anwendungskonnektors	**Beschreibung**	**Sicherheitsattribut**
		C.eGK.AUT_CVC[33] als eGK gegenüber anderen Chipkarten, - SK.CMS[34] als eGK gegenüber einem CMS, - SK.VSD[35] 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[36], Träger des Entschlüsselungsschlüssels und PIN-Empfänger.	Identität: - ICCSN - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten und Entschlüsselungsschlüsselinhabers für zu verschlüsselnde Daten.[37] Authentisierungsreferenzdaten mit Rollenkennung: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten - C.HPC.AUTR_CVC[38] als HBA gegenüber SMC und eGK, - C.HPC.AUTD_SUK_CVC[39]als QSEE für Stapelsignatur und PIN-Empfänger - C.HP.ENC als Träger des dazu gehörigen Entschlüsselungsschlüssels PrK.HP.ENC.

[33] C.eGK.AUT_CVC steht hier für C.eGK.AUT_CVC.R2048 und C.eGK.AUT_CVC.E256 sowie den optionalen C.eGK.AUT_CVC.E384 der Spezifikation des Objektsystems der eGK [98].

[34] SK.CMS steht hier für SK.CMS.AES128 und den optionalen SK.CMS.AES256 der Spezifikation des Objektsystems der eGK [98].

[35] SK.VSD steht hier für SK.VSD.AES128 und den optionalen SK.VSD.AES256 der Spezifikation des Objektsystems der eGK [98].

[36] PrK.HP.QES steht hier für PrK.HP.QES.R2048 und die optionalen PrK.HP.QES.R3076 der Spezifikation des Objektssystems [99].

[37] Durch organisatorische Maßnahmen ist sicherzustellen, dass die Identität des Benutzers des Clientsystems und die Identität des Signaturschlüssel-Inhabers der zu signierenden Daten eindeutig einander zugeordnet wird.

[38] C.HPC.AUTR_CVC steht hier für C.HPC.AUTR_CVC.R2048 und C.HPC.AUTR_CVC.E256 sowie den optionalen C.HPC.AUTR_CVC.E384 der Spezifikation des Objektsystems des HBA [99].

[39] C.HPC.AUTD_SUK_CVC steht hier für C.HPC.AUTD_SUK_CVC.R2048 und C.HPC.AUTD_SUK_CVC.E256 sowie den optionalen C.HPC.AUTD_SUK_CVC.E384 der Spezifikation des Objektsystems des HBA [99].

Benutzer des Anwendungskonnektors	**Beschreibung**	**Sicherheitsattribut**
		Optionale Authentisierungsreferenzdaten[40]: - 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[41] als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC[42] als SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung. Optionale Authentisierungsreferenzdaten[43]:

[40] Gemäß der Spezifikation des Objektsystems des HBA [99], Kap. 5.3.16 und 5.3.17, müssen die Objekte bei der Initialsierung angelegt und bei der Personalisierung nur die Schlüssel personalisiert werden, die tatsächlich benötigt werden. Sie werden für die Kartenadministration durch das CMS genutzt. Die asymmetrische Kartenadministration setzt asyemtrische Schlüsselpaare der Karte voraus. Die symmetrische Kartenadministration erfordert einen gegenseitige Authentisierung mit MUTUAL AUTHENTICATION zwischen Karte und CMS.

[41] C.SMC.AUTR_CVC steht hier für C.SMC.AUTR_CVC.R2048 und C.SMC.AUTR_CVC.E256 sowie den optionalen C.SMC.AUTR_CVC.E384 der Spezifikation des Objektsystems der SMC-B [100]

[42] C.SMC.AUTD_RPE_CVC steht hier für C.SMC.AUTD_RPE_CVC.R2048, C.SMC.AUTD_RPE_CVC.E256 und den optionalen C.SMC.AUTD_RPE_CVC.E384 der Spezifikation des Objektsystems der gSMC-KT [102] bzw. der SMC-B [100]

[43] Gemäß der Spezifikation des Objektsystems der SMC-B [100], Kap. 5.3.15 und 5.3.16, müssen die Objekte bei der Initialsierung angelegt und bei der Personalisierung nur die Schlüssel personalisiert werden, die tatsächlich benötigt werden. Sie werden für die Kartenadministration durch das CMS genutzt. Die asymmetrische Kartenadministration setzt asyemtrische

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
		- PuK.RCA.ADMINCMS.CS.E256 des CMS gegenüber einer SMC-B. - 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[44] als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC[45] als SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung,.

Tabelle 7: 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[46])
KT-Benutzer	Benutzer des eHealth-Kartenterminals.

Tabelle 8: Benutzer anderer Komponenten in der IT-Umgebung

Schlüsselpaare der Karte voraus. Die symmetrische Kartenadministration erfordert einen gegenseitige Authentisierung mit MUTUAL AUTHENTICATION zwischen Karte und CMS.

[44] C.SMC.AUTR_CVC steht hier für C.SMC.AUTR_CVC.R2048 und C.SMC.AUTR_CVC.E256 sowie den optionalen C.SMC.AUTR_CVC.E384 der Spezifikation des Objektsystems der SMC-B [100]

[45] C.SMC.AUTD_RPE_CVC steht hier für C.SMC.AUTD_RPE_CVC.R2048, C.SMC.AUTD_RPE_CVC.E256 und den optionalen C.SMC.AUTD_RPE_CVC.E384 der Spezifikation des Objektsystems der gSMC-KT bzw. der SMC-B [100]

[46] MRPIN.home wird nur außerhalb der TI verwendet.

3.2. Bedrohungen

3.2.1. Gegen den Netzkonnektor gerichtete Bedrohungen

Die folgenden Bedrohungen sind dem Schutzprofil BSI-CC-PP-0097-V2 [77] entnommen:

3.2.1.1. Auswahl der betrachteten Bedrohungen

Eine Motivation der in Abschnitt 3.2.1 beschriebenen Bedrohungen sowie eine Beschreibung der möglichen Angriffspfade ist dem BSI-CC-PP-0097-V2 [77], Abschnitt 3.3.1, zu entnehmen und wird in diesem Security Target nicht wiederholt. Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen werden wie folgt zusammengefasst:

- 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 Leistungserbringers 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 Leistungserbringers 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.

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

3.2.1.2. Liste der Bedrohungen

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

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt. Das Kästchen „LAN-Interface“ stellt entweder die Verbindung zum Anwendungskonnektor dar oder schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

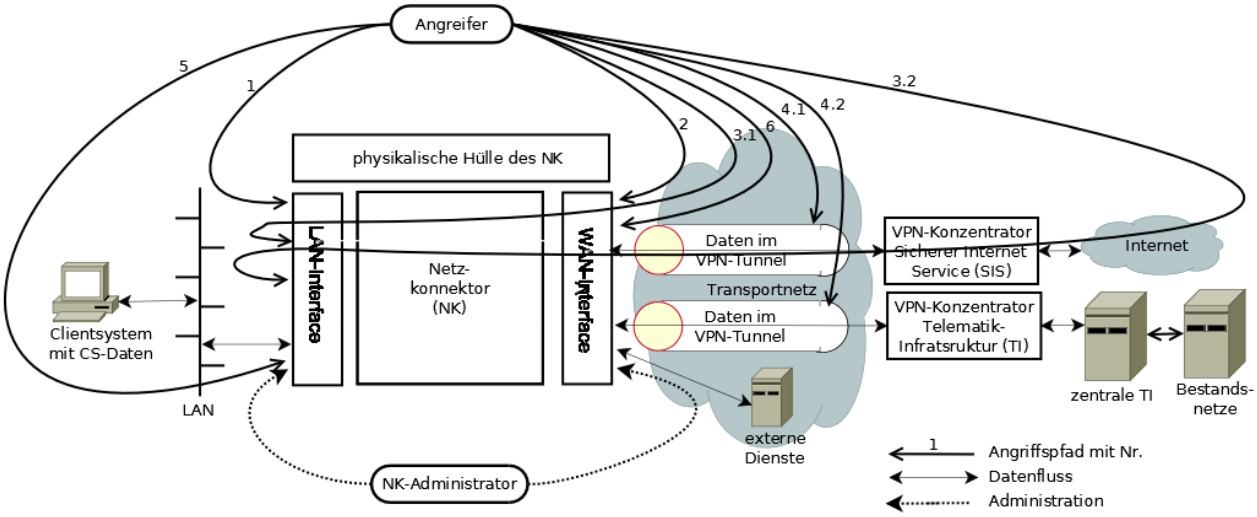


Abbildung 7: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

Zusätzlich zu den in Abbildung 7 visualisierten Angriffspfaden (Nr. 1 bis Nr. 6) bzw. den zugeordneten Bedrohungen könnte ein Angreifer

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

Die Bedrohungen werden im restlichen Dokument mit den folgenden Bezeichnern referenziert und sämtlich innerhalb dieses Abschnitt beschrieben:

Angriffspfad	Bezeichner
Nr. 1	T.NK.local_EVG_LAN
Nr. 2	T.NK.remote_EVG_WAN
Nr. 3.1	T.NK.remote_EVG_LAN
Nr. 3.2	T.NK.remote_EVG_LAN
Nr. 4.1	T.NK.remote_VPN_Data
Nr. 4.2	T.NK.remote_VPN_Data
Nr. 5	T.NK.local_admin_LAN
Nr. 6	T.NK.remote_admin_WAN
Konnektornachbauten	T.NK.counterfeit
Zertifikatsstatusabfragen	T.NK.Zert_Prüf
Zeitsynchronisation	T.NK.TimeSync
DNS-Manipulation	T.NK.DNS

Tabelle 9: Kurzbezeichner der Bedrohungen

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

berechtigten Zugang zu vor physischen Zugriff geschützten Bereichen des Leistungserbringers haben, entweder vertrauenswürdig[47] sind (so dass von ihnen keine Bedrohungen ausgehen, z. B. Arzt selbst, Servicetechniker, einige Angestellte) oder dass der physische Zugriff durch den Leistungserbringer geeignet beschränkt wird (z. B. Patienten dürfen zwar Wartezimmer und Behandlungsräume betreten, aber nicht auf den gesicherten Bereich zugreifen in welchem der Konnektor aufbewahrt wird – siehe die Annahme A.AK.phys_Schutz).

Die Angriffe, deren Bezeichner das Wort „remote“ enthalten (T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.remote_VPN_Data und T.NK.remote_admin_WAN), nehmen an, dass der Angreifer über keinen solchen physischen Zugriff auf Geräte erlangt, sondern dass die Angriffe ausschließlich über das Transportnetz (z. B. Internet) erfolgen.

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

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[48], 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.).

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

[48] Personal Digital Assistant

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

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 Abschnitt 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 Abschnitt 0 T.NK.local_EVG_LAN beschrieben. Im Gegensatz zur Bedrohung T.NK.remote_EVG_WAN ist das Ziel jedoch nicht, den Netzkonnektor direkt an seiner WAN-Schnittstelle anzugreifen, sondern über den Netzkonnektor zunächst Zugriff auf das lokale Netz des Leistungserbringers (LAN) zu erhalten, um dort ein Clientsystem zu kompromittieren und möglicherweise im Anschluss daran den Konnektor von dessen LAN-Seite her anzugreifen. Die Kompromittierung eines Clientsystems ist gegeben, wenn ein Angreifer aus dem Transportnetz bzw. dem Internet unautorisiert auf personenbezogene Daten im Clientsystem zugreifen kann oder wenn der Angreifer ein Clientsystem erfolgreich und unbemerkt manipulieren kann.

Hierzu werden in Abbildung 7 zwei Angriffspfade unterschieden:

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[49] zwischen WAN und LAN leistet.

Betroffene zu schützende Werte sind:

- zu schützende Daten der TI und der Bestandsnetze während der Übertragung
- zu schützende Nutzerdaten während der Übertragung
- zu schützende Daten der TI und der Bestandsnetze im Clientsystem
- Clientsystem, Anwendungskonnektor
- zu schützende Daten der TI und der Bestandsnetze im Netzkonnektor

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

- 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 aus Abbildung 7) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 7) 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[50]). 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[51]. 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.

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-Verteilungspunkts manipulieren oder sich selbst als dieser Verteilungspunkt ausgeben.

[50] Der vorliegende EVG unterstützt die Remote Administration nicht. Diese Bedrohung verbleibt wegen strikter Konformität zum unterliegenden PP in diesen Sicherheitsvorgaben.

[51] 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.

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.

T.NK.DNS

Ein Angreifer manipuliert aus dem Transportnetz heraus Antworten auf DNS-Anfragen zu externen DNS-Servern. Dies kann einerseits Anfragen des Netzkonnektors betreffen, wenn dieser vor dem Aufbau von VPN-Kanälen die Adresse des VPN-Konzentrators der TI oder des SIS ermitteln will. Im Ergebnis wird keine oder eine falsche Adresse ausgeliefert, so dass der Netzkonnektor ggf. die VPN-Verbindung zu einem gefälschten Endpunkt aufbaut, der beispielsweise eine gefälschte zentrale TI-Plattform vorspiegelt. Dadurch werden die zu schützenden 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 hinaus definiert das Schutzprofil die folgenden weiteren Bedrohungen gegen die zu schützenden Werte.

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 Zeitdienst, kann diesen Dienst manipulieren oder verhindern. Damit wird der EVG mit gefälschten PKI- oder Zeitinformationen versorgt oder die PKI- oder Zeitinformationen 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

OSP.NK.Zeitdienst Zeitdienst

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

OSP.NK.SIS Sicherer Internet Service

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

OSP.NK.BOF Kommunikation mit Bestandsnetzen und offenen Fachdiensten

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

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

Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*]. Zudem prüft der EVG die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

OSP.NK.SW-Update Software-Update

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

Es dürfen nur von einer autorisierten Stelle geprüfte, freigegebene und ggf. zertifizierte Komponenten bzw. Fachmodule zum Update bereit gestellt werden. Der Administrator hat im Zertifizierungsfall darauf zu achten, dass nur die gemäß des Zertifizierungsreports ausgewiesenen technischen Komponenten zum Einsatz kommen.

Bevor ein Software-Update installiert wird, wird die Integrität und Authentizität / Zulässigkeit der Software überprüft (Signaturprüfung und Prüfung der Identität des Signierenden, Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen). Schlägt die Prüfung der Integrität fehl, verhindert der EVG eine Aktualisierung der Software. Falls das Aktivieren einer neuen Software-Version fehlschlägt, wird der letzte funktionierende Software-Stand der Komponente reaktiviert.

Hinweis: OSP.NK.SW-Update wurde von OSP.AK.SW-Update aus dem Protection Profile [78] abgeleitet.

3.3.2. Organisatorische Sicherheitspolitiken des Anwendungskonnektors

Die organisatorischen Sicherheitspolitiken 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 [8].

3.3.2.1. allgemeine organisatorische 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 [90] und der Spezifikation Konnektor [92]. 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. Dieses Security Target verweist in Anlehnung an das zugrundeliegende BSI-CC-PP-0098-V3 auf diese Beschreibungen, soweit dies für die Festlegung von Sicherheitseigenschaften erforderlich ist. Eine Produktevaluierung gemäß dieser Sicherheitsvorgaben stellt auch fest, dass Funktionen des EVG den Sicherheitsanforderungen dieses Schutzprofils nicht widersprechen.

OSP.AK.KryptAlgo Kryptographische Algorithmen

Alle kryptographischen Sicherheitsmechanismen der technischen Komponenten der Telematikinfrastruktur werden im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*] implementiert. Für den Signaturdienst für qualifizierte elektronische Signaturen gelten die Festlegungen gemäß [9].

OSP.AK.SW-Update Software-Update

Die Software des Konnektors 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 zu unterscheiden.

Es dürfen nur von einer autorisierten Stelle geprüfte, freigegebene und ggf. zertifizierte Komponenten bzw. Fachmodule signiert und zum Update bereit gestellt 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[52]). 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 Vorgänge und auf entsprechende Nutzer zu beschränken. Ebenso müssen Aktualisierungen protokolliert 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.

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.

[52] Einspielen älterer Software-Versionen ist nur dann erlaubt, wenn die einzuspielende Version in der aktuell gültigen Liste zulässiger Software-Versionen (Firmware-Gruppe) ist (siehe [103]).

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_DataUnversehrtheit 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, die Kommunikation mit dem zentralen Verzeichnisdienst, die Kommunikation mit der VAU des ePA Aktensystems und die Kommunikation mit dem Schlüsselgenerierungsdienst SGD. 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.

3.4. Annahmen

3.4.1. Annahmen an den Netzkonnektor

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

Die Sicherheitsmaßnahmen in der Umgebung schützen den Konnektor (während aktiver Datenverarbeitung im Konnektor) vor physischem 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.

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: 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: Siehe auch [77], Abschnitt 7.6.8.

A.NK.AK Anwendungskonnektor nutzt EVG korrekt

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

Anwendungshinweis 28: Der Konnektor ist modular aufgebaut. Die einzelnen Module werden durch einen Security and Separation Layer (Virtualisierungsschicht) separiert. Neben der Hardware-Virtualisierung laufen die Module jeweils in eigenen Betriebssystems-Anwendungscontainern (Linux Container Umgebung). Die Kommunikation der Module untereinander wird durch ein dediziertes Firewall Modul geregelt. Daten die an die zentrale TI-Plattform und an den SIS weitergeleitet werden, sind daher strikt getrennt.

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 Konnektor ist modular aufgebaut. Die einzelnen Module werden durch einen Security and Separation Layer (Virtualisierungsschicht) separiert. Neben der Hardware-Virtualisierung laufen die Module jeweils in eigenen Betriebssystems-Anwendungscontainern (Linux Container Umgebung). Die Kommunikation der Module untereinander wird durch ein dediziertes Firewall Modul geregelt. Daten die an die zentrale TI-Plattform und an den SIS weitergeleitet werden, sind daher strikt getrennt.

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 [78] 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 in BSI-CC-PP-0098-V3 [78] des Gesamtkonnektors als übergreifende Sicherheitsfunktion modelliert.

3.4.2. Annahmen an den Anwendungskonnektor

Die folgenden Abschnitte enthalten zusätzliche Annahmen für den EVG des vorliegenden Schutzprofiles.

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 vertrauenswürdig.

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 Konnektors 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, erfolgt auf technischem Wege. Das Handbuch des EVG enthält einen entsprechenden Hinweis enthalten, dass die genutzte Firmware-Version im Primärsystem angezeigt wird. Außerdem enthält der Hinweis folgende Aspekte:

- Der Nutzer muss im Falle automatischer Updates prüfen, ob die genutzte Firmware-Version geeinet ist, d.h. ob diese von der gematik zugelassen ist.
- Bei einem Update wird die Konfiguration des Paramaters zum automatischen Update nicht auf „enabled“ geändert, wenn er vor dem Update „disabled“ war.

- Der Administrator kann – wenn er dies möchte – die Konfiguration so wieder ändern, ohne dass bereits ungewollt automatische Updates stattfinden.

Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartententerminals organisatorisch geschützt werden. Dies gilt auch für ein automatisches Update. Die Guidance informiert den Administrator darüber, damit dieser den Nutzer informieren kann bzw. ein Zeitraum für automatische Updates konfiguriert wird, an dem der organisatorische Schutz per se gegeben ist.

A.AK.Cardterminal_eHealth Nutzung eines sicheren Kartenterminals

Für die Chipkarten und die Eingabe von Benutzerverifikationsdaten werden ausschließlich eHealth-Kartenterminals verwendet, die der Spezifikation [94] entsprechen und nach dem Schutzprofil für eHealth-Kartenterminals [80] evaluiert wurden.

A.AK.Konnektor Konnektor

Die Anwender/Benutzer setzen nur solche Konnektoren ein, welche der Spezifikation [92] entsprechen und nach dem Konnektor Schutzprofil BSI-CC-PP-0098-V3 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 [97] entspricht und nach dem Schutzprofil COS Schutzprofil [79] evaluiert ist und dessen Objektsysteme der Spezifikation [100] bzw. [102] 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 [97] entspricht und nach dem Schutzprofil COS [79] evaluiert ist, deren Objektsysteme der Spezifikation [99] entspricht und das als qualifizierte elektronische Signaturerstellungseinheit nach eIDAS zertifiziert ist.

Anwendungshinweis 32: Gemäß Spezifikation [99] 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 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 Netzkonnektor.

4. Sicherheitsziele

4.1. Sicherheitsziele für den Netzkonnektor

Dem Schutzprofil BSI-CC-PP-0097-V2 [77] sind folgende Sicherheitsziele für den Netzkonnektor entnommen:

4.1.1. Allgemeine Ziele: Schutz und Administration

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

Der EVG stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*]. Zudem prüft der EVG 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 EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten. Der EVG schützt sich selbst gegen sicherheitstechnische Veränderungen an den äußeren logischen Schnittstellen bzw. erkennt diese oder macht diese erkennbar.

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

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

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

Anwendungshinweis 34: Annahmen zum physischen Schutz: Der Schutz vor physischen Angriffen wird durch die Einsatzumgebung gewährleistet (siehe A.AK.phys_Schutz). Der EVG selbst besteht nur aus der Software des Netzkonnektors.

O.NK.EVG_Authenticity Authentizität des EVG

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

Anwendungshinweis 35: Die Auslieferung des Konnektors zum empfangenden Leistungserbringer oder dem von ihm beauftragten Servicetechniker erfolgt durch gesicherten Transport. Nach Erhalt des Konnektors 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 [10] authentisiert hat und fachliche Anwendungsfälle im Online-Modus durchgeführt werden können.

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

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

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

Weil die Administration über Netzverbindungen (lokal über PS1) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).

Der EVG verhindert die Administration folgender Firewall-Regeln:

- Regeln für die Kommunikation zwischen Konnektor und Transportnetz,
- Regeln für die Kommunikation zwischen Konnektor und Telematikinfrastruktur, 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 wird TOE intern zwischen den zwei Administrator-Rollen *local administrator* und *super administrator* unterschieden. Der lokale Administrator kann den EVG über die LAN- Schnittstelle konfigurieren. Der Super Adminsistrator hat kann zudem die Benutzerkonten verwalten. Dazu gehört die Vergabe von Zugriffsrechten bezüglich der Konfigurationsbereiche und zum Werksreset. Auch die Super-Administration erfolgt über die lokale Schnittstelle (LAN). Es können alle Management-Funktionen der TSF von den beiden Administrator-Rollen ausgeführt werden. Daher werden unter dem Subjekt Administrator die einzelnen Rollen zusammengefasst. Der EVG nimmt die Authentisierung selbst vor; O.NK.Admin_EVG wurde aus BSI-CC-PP-0097-V2 [77] übernommen und geeignet verschärft. Die Anpassungen gegenüber dem Schutzprofil wurden durch durchgestrichenen Text kenntlich gemacht.

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

Anwendungshinweis 38: Der für die Administration notwendige sichere logische Kanal beruht auf den durch [*86*] vorgegebenen Protokollen und Algorithmen.

O.NK.Admin_Auth Der Netzkonnektor führt die Authentisierung des Administrators durch.

Der EVG 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, automatisch ablaufender Signatur- und Verschlüsselungsprozesse der Anwendungen und die Aktivierung und Deaktivierung der Online Kommunikation, des Signaturdienstes und der Logischen Separation. Die Administration erfolgt über eine Managementschnittstelle. Der EVG erzwingt die bezüglich Vertraulichkeit und Integrität geschützte Kommunikation zur Administration über die Managementschnittstelle.

Hinweis: O.NK.Admin_Auth wurde von O.AK.Admin aus dem Protection Profile BSI-CC-PP-0098-V3 [78] übernommen und hier als Sicherheitsziel des Netzkonnektors bezeichnet.

O.NK.Protokoll Protokollierung mit Zeitstempel

Der EVG 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 EVG synchronisiert die Echtzeituhr gemäß OE.AK.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 EVG oder andere Komponenten bereitgestellt werden, muss die Integrität und die Authentizität / Zulässigkeit der Updatedaten überprüft (Signaturprüfung und Prüfung der Identität des Signierenden) und Metadaten (zum Schutz gegen unbefugtes Wiedereinspielen älterer Software-Versionen) angezeigt werden. Schlägt die Prüfung der Integrität fehl, verhindert der EVG die Bereitstellung der Updatedaten. Die Installation dieser Updates 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 BSI-CC-PP-0098-V3 [78] abgeleitet und bezieht sich auf das Update der Software des Konnektors, nicht jedoch auf die Updates von TSL, CRL und BNetzA-VL. Die Updatefunktion für Software wird komplett durch den Netzkonnektor implementiert und daher wurden alle SFRs, die laut BSI-CC-PP-0098-V3 [78], Abschnitt 6.5.5 dem Aspekt Update der Software zugeordnet sind, in diesen Sicherheitsvorgaben aus Konsistenzgründen tw. umbenannt. Im Einzelnen sind diese SFRs in der folgenden Tabelle gelistet:

Bezeichner in BSI-CC-PP-0098-V3 **[78]**	**Bezeichner in diesen Sicherheitsvorgaben**
FDP_ACC.1/AK.Update	FDP_ACC.1/NK.Update
FDP_ACF.1/AK.Update	FDP_ACF.1/NK.Update
FDP_UIT.1/AK.Update	FDP_UIT.1/NK.Update
FTP_ITC.1/AK.KSR	FTP_ITC.1/AK.KSR

4.1.2. Ziele für die VPN-Funktionalität

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

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

- Der EVG prüft zertifikatsbasiert die Authentizität der VPN-Konzentratoren der TI und des SIS.
- Der EVG 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 der Bundesregierung*, Teil 1: Telematikinfrastruktur [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*] noch gültig sind.

Anwendungshinweis 42: Der EVG implementiert die Algorithmen nach Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur [76]. Eine Prüfung der Gültigkeit der Algorithmen wird nicht explizit durchgeführt. Die Gültigkeit wird im Rahmen der Evaluierung des Netzkonnektors sichergestellt. Weiterhin bietet der EVG keine Funktionalität die Verfügbarkeit der in Bezug auf die benannten Spezifikationen ungültigen Algorithmen selektiv einzuschränken. Eine Einschränkung der im Konnektor verwendbaren Algorithmen wird über ein Software-Update durchgesetzt.

O.NK.Zert_Prüf Gültigkeitsprüfung für VPN-Zertifikate

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

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

Der EVG schützt die Vertraulichkeit der Nutzdaten[53] bei der Übertragung von und zu den VPN-Konzentratoren.

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

Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.

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

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

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

4.1.3. Ziele für die Paketfilter-Funktionalität

O.NK.PF_WAN Dynamischer Paketfilter zum WAN

Der EVG schützt sich selbst und andere Konnektorteile vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN). Wenn der Konnektor das einzige Gateway vom LAN der Leistungserbringer zum Transportnetz darstellt[54], dann schützt der EVG auch die Clientsysteme.

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

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

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

O.NK.PF_LAN Dynamischer Paketfilter zum LAN

Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN). Es werden Angreifer mit hohem Angriffspotential betrachtet.

Für zu schützende Daten der TI und der Bestandsnetze sowie *zu schützende Nutzerdaten* bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels.

---

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

54 Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [**Fehler! Textmarke nicht definiert.**], Kapitel 2.7.

Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Clientsystemen) auf das Transportnetz wird durch den EVG unterbunden: IT-Systeme im LAN können nur unter der Kontrolle des EVG und im Einklang mit der Sicherheitspolitik des EVG zugreifen.

Anwendungshinweis 44: Siehe auch OE.NK.AK.

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

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

4.2. Sicherheitsziele für den Anwendungskonnektor

Über die in Abschnitt 4.1 aufgeführten Sicherheitsziele 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 [9] und für alle anderen Kryptoverfahren des AK gemäß [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*].

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 AK 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 [92], 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 AK 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 AK 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 AK mit den Inhalten der bezogenen Listen aktualisiert.

Der beschriebene Update-Vorgang für die Software des AK bezieht explizit die Software des Netzkonnektors mit ein. Die Updatefunktion für Software und freigegebene Fachmodule ist komplett im Anteil Netzkonnektor zu implementiert. Zu diesem Zweck wurde das Sicherheitsziel O.AK.Update aus BSI-CC-PP-0098-V3 in O.NK.Update umbenannt und der Funktionalität des Netzkonnektors zugeordnet, siehe Abschnitte 6.2.6 und 7.1.6.

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 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 [26] [44] sowie zusätzlich für PDF/A gemäß PAdES [27] [45] und für XML zusätzlich XAdES [25] [43].

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.

Hinweis: O.AK.Sig.SignQES beinhaltet die Prüfung auf Wohlgeformtheit der zu signierenden Dokumente gegen die entsprechende Format-Spezifikation. Für Fachmodule bedeutet dies insbesondere, dass die Prüfung gegen das in der Signaturrichtline festgelegte XML Schema stattfindet.

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, XML und von binären Dokumente sowie für Binärstrings[55]. 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 [75] 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.

[55] Dies entspricht dem Stand der Liste unterstützter Formate zum Zeitpunkt der Erstellung des Schutzprofiles. Der ST Autor soll die gültige Liste nach der jeweils aktuellen Konnektor-Spezifikation [**Fehler! Textmarke nicht definiert.**] verwenden

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 [75]. 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.

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. [75]).

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: Dieses PP betrachtet ausschließlich die Einfach- und die Stapelsignatur. Sollen vom EVG weitere Signaturarten – wie bspw. die Komfortsignatur – umgesetzt werden, ist das ST in Abstimmung mit der Zertifizierungsstelle entsprechend zu erweitern. In der vorliegenden Produktversion wird die Komfortsignatur umgesetzt und sind die dazu erforderlichen Inhalte in das Security Target aufgenommen worden.

O.AK.Sig.Komfortsignatur Komfortsignatur

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen durch eine Komfortsignatur gemäß [93].

Der AK steuert die lokale oder entfernte Eingabe der QES-PIN am eHealth Kartenterminal für die Freischaltung des HBA für die Komfortsignatur. Der AK authentisiert sich gegenüber dem HBA mit der Identität „SAK“. Die Kommunikation zwischen AK und HBA ist per Secure Messaging geschützt. Das Clientsystem authentisiert sich für die Signaturerzeugung mit derjenigen UserID beim AK, die zur Freischaltung der Komfortsignatur verwendet wurde.

Der AK kontrolliert die Erzeugung qualifizierter elektronischer Signaturen für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten. Dabei obliegt es dem Clientsystem sicherzustellen, dass eine Signatur im Rahmen einer Komfortsignatur durch den autorisierten Benutzer ausgelöst wird (vgl. OE.AK.Clientsystem). Bei festgestellten Abweichungen im Signaturprozess wird das Clientsystem über die Schnittstellen darüber informiert und die Signaturen der Daten verworfen. Der AK setzt den Sicherheitszustand des HBA, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers erlangt wurde, zurück, wenn die eingestellte maximale Anzahl von Komfortsignaturen bzw. das Ende des konfigurierten Zeitintervalls erreicht wurde, oder wenn die Funktion zur Erstellung von Komfortsignaturen durch den Benutzer oder einen Administrator deaktiviert wurde.

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 [9]. 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 [76] 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.

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.

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.

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 [92] 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.[56] 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.

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

[56] 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.

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 [34], XML-Encryption [21] und S/MIME [35] 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.

O.AK.VAU Kommunikation mit der VAU des ePA Aktensystems

Der Konnektor stellt einen gesicherten Kanal zwischen dem EVG und der vertrauenswürdigen Ausführungsumgebung (VAU) bereit und ermöglicht damit den spezifikationskonformen Zugriff auf die VAU durch das Fachmodul ePA.

O.AK.SGD Kommunikation mit dem SGD

Der Konnektor stellt einen gesicherten Kanal zwischen dem EVG und dem HSM des Schlüsselgenerierungsdienstes (SGD) bereit und ermöglicht damit den Empfang von kryptographischem Material im Zusammenhang mit den Anwendungsfällen des Fachmodul ePA.

4.3. Sicherheitsziele für die Umgebung des Netzkonnektors

OE.NK.RNG Externer Zufallszahlengenerator

Die Umgebung stellt dem EVG einen externen Zufallszahlengenerator bereit, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klassen PTG.2 oder PTG.3 aus [7] 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.

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-Platform des Netzkonnektors muss eine Real Time Clock mit maximale zulässigem Fehler von +/- 20ppm (part per million) zur Verfügung stellen. 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-0097-V2 [77] des Netzkonnektors entnommen und ist nur zur Vollständigkeit in hier enthalten. 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.AK.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 EVG verwendet nur von der gematik zugelassene Sicherheitsmodule gSMC-K.

OE.NK.KeyStorage Sicherer Schlüsselspeicher

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

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

Anwendungshinweis 58: Der Netzkonnektor stellt ein symmetrisch verschlüsseltes Filesystem (Crypted File System, CFS) als Datenspeicher für sichere Speicherung von Geheimnissen zur Verfügung. Der symmetrische Schlüssel selbst wird durch einen asymmetrischen Schlüssel der in der gSMC-K („sicherer Schlüsselspeicher“) hinterlegt ist geschützt.

Anwendungshinweis 59: Der Schlüsselspeicher wird auch zur Speicherung von

- Geheimnissen (Passwörtern), mit denen der Administrator sich gegenüber dem EVG authentisieren kann (FTP_TRP.1/NK.Admin), sowie vom
- DNSSEC Vertrauensanker der TI (DNSSEC wird vom DNS-Dienst des EVG unterstützt)

verwendet.

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 [10] 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.AK.Konnektor.

Anwendungshinweis 61: Das Umgebungsziel des Netzkonnektors OE.NK.AK ist der Struktur von BSI-CC-PP-0098-V3 [78] folgend von BSI-CC-PP-0097-V2 [77] übernommen worden und nur der Vollständigkeit halber enthalten. Vgl. 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 [10] korrekt aufrufen. Aufrufe von Diensten gemäß § 291a SGB V [10] 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 abhandenkommt, 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 hat eine Seriennummer, über die eine Identifikation erfolgen kann. 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 und weitergehende Schritte (z. B. Sperrung des zugehörigen Zertifikats) eingeleitet werden können.

OE.NK.Admin_Auth Authentisierung des Administrators

Entfällt in diesen Sicherheitsvorgaben, siehe Anwendungshinweis 63.

Anwendungshinweis 63: Der EVG führt die Authentisierung selbst durch. Das Umgebungsziel OE.NK.Admin_Auth aus dem PP [77] wurde in ein EVG-Ziel O.NK.Admin_Auth umgewandelt und wird in diesem ST daher nicht mehr aufgeführt. OE.NK.Admin_Auth kann als automatisch durch O.NK.Admin_Auth und O.AK.Admin erfüllt angesehen werden. Die funktionale Anforderung FMT_MSA.4/NK wird beibehalten, da die Anforderung, dass nur bei erfolgreicher Autorisierung ein entsprechender Sicherheitszustand gesetzt wird, nach wie vor gültig ist.

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 abhandengekommen, so sperrt der Betreiber der PKI das zugehörige Zertifikat und stellt diese Information (über eine CRL) für die VPN-Konzentratoren bereit, so dass diese mit dem abhanden gekommenen Konnektor keine Verbindung mehr aufbauen.

OE.NK.phys_Schutz Physischer Schutz des EVG

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

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

Anwendungshinweis 64: Siehe auch A.AK.phys_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-0097-V2 [77] des Netzkonnektors entnommen und ist nur der Vollständigkeit halber enthalten. 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 Clientsysteme

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.[57]

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[58] 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 EVG nur dann signiert und ausgeliefert werden, wenn der Code von einer dazu autorisierten Stelle geprüft und freigegeben wurde. Zertifizierte EVG-Komponenten dürfen nur durch zertifizierte Komponenten ersetzt werden.

Hinweis: OE.NK.SW-Update wurde von OE.SW-Update aus dem Protection Profile BSI-CC-PP-0098-V3 [78] abgeleitet.

Die vorgenannten Sicherheitsziele für die Umgebung aus [77] werden der Struktur von BSI-CC-PP-0098-V3 [78] folgend in diesem ST in anderer Weise umgesetzt. Tabelle 10 enthält diese Sicherheitsziele zusammen mit der Erklärung, wie sie in diesem ST behandelt werden.

Sicherheitsziel aus BSI-CC-PP-0097-V2 [77]	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-V2 [77] des Netzkonnektors entnommen und ist nur zur Vollständigkeit enthalten. Die korrekte Nutzung der NK-Schnittstellen durch den AK ist im Rahmen der Evaluierung des EVG zu prüfen (u.a. CC-Klassen ADV und ATE).
OE.NK.Admin_Auth	Das Umgebungsziel OE.NK.Admin_Auth aus dem Protection Profile BSI-CC-PP-0097-V2 [77] wurde in das Sicherheitsziel O.NK.Admin_Auth des EVG umgewandelt.

[57] Es wird darauf hingewiesen, dass ein absoluter Schutz der Netze vor Angriffen aus dem Internet durch einen gesicherten Zugangspunkt praktisch nicht realisierbar ist. Als Folge muss der Schutz der Clientsysteme stets auch weitere Maßnahmen umfassen. In diesem Security Target wird daher eine Kombination aus einem gesicherten Zugangspunkt zum Internet (OE.NK.SIS) und lokalen Schutzmaßnahmen auf den Clientsystemen (OE.NK.Betrieb_CS) gefordert.

[58] Laut Konnektor-Spezifikation (Kapitel 2.7) [**Fehler! Textmarke nicht definiert.**] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

Sicherheitsziel aus BSI-CC-PP-0097-V2 [77]	Bemerkungen
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 ür 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 im Rahmen der Evaluierung des EVG zu prüfen.
OE.NK.phys_Schutz	Physischer Schutz des EVG. A.NK.phys_Schutz und A.AK.phys_Schutz sind identisch formuliert. OE.NK.phys_Schutz und OE.AK.phys_Schutz sind ebenfalls identisch formuliert. A.NK.phys_Schutz und 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 Abschnitt 4.3 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 die kryptographischen Vorgaben aus [76] 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 und 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 BSI TR-03116-1 [76] 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 Konnektors 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 genutzten Konnektorfirmware-Version zu prüfen.

Anwendungshinweis 69: Die Information der Benutzer des AKs, welche Firmware-Version aktuell genutzt wird, erfolgt auf technischem Wege. Das Handbuch des EVG enthält einen entsprechenden Hinweis enthalten, dass die genutzte Firmware-Version im Primärsystem angezeigt wird. Außerdem enthält der Hinweis folgende Aspekte:

- Der Nutzer muss im Falle automatischer Updates prüfen, ob die genutzte Firmware-Version geeinet ist, d.h. ob diese von der gematik zugelassen ist.
- Bei einem Update wird die Konfiguration des Paramaters zum automatischen Update nicht auf „enabled“ geändert, wenn er vor dem Update „disabled“ war.
- Der Administrator kann – wenn er dies möchte – die Konfiguration so wieder ändern, ohne dass bereits ungewollt automatische Updates stattfinden.

Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartententerminals organisatorisch geschützt werden. Dies gilt auch für ein automatisches Update. Die Guidance informiert den Administrator darüber, damit dieser den Nutzer informieren kann bzw. ein Zeitraum für automatische Updates konfiguriert wird, an dem der organisatorische Schutz per se gegeben ist.

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 [80] 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, und

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

(7) die Vorgaben der BSI TR-03116-1 [76] 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 [79] 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 [76].

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 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.

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 [79] 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 [76] 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 [79] und der Spezifikation des Objektsystems [98] 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 [76] 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.

Im Rahmen der Komfortsignatur stellt das Clientsystem sicher, dass die dabei verwendete UserID sicher und korrekt erzeugt wird und der Benutzer vor jedem Auslösen einer Komfortsignatur authentisiert wird (vgl. auch A_19101 in [93]).

Alle genutzten kryptographischen Sicherheitsmechanismen werden im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 [76] implementiert.

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 [92] 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 EVG und die Umgebung ab.

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.AK.Basis_Krypto	O.NK.Schutz	O.NK.FVG_Authenticity	O.NK.Admin_FVG	O.AK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	O.NK.Admin_Auth	OE.NK.RNG	OE.AK.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.nhvs_Schutz	OE.AK.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	

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.AK.Basis_Krypto	O.NK.Schutz	O.NK.FVG_Authenticity	O.NK.Admin_FVG	O.AK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	O.NK.Admin_Auth	OE.NK.RNG	OE.AK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.gSMC-K	OE.NK.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_FVG	OE.NK.PKI	OE.NK.phys_Schutz	OE.AK.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.remote_VPN_Data						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									
T.NK.remote_admin_WAN		X		X	X	X									X	X	X	X		X			X									
T.NK.counterfeit			X																X						X							
T.NK.Zert_Prüf									X															X							X		
T.NK.Time Sync						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.AK.phys_Schutz																									X							
A.NK.gSMC-K																			X													
A.AK.sichere_TI																										X						
A.NK.kein_DoS																											X					
A.AK.Konnektor																					X											
A.NK.CS																						X										
A.NK.Betrieb_AK																												X				
A.NK.Betrieb_CS																													X			

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.AK.Basis_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.AK.Protokoll	O.NK.Zeitdienst	O.NK.Update	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	O.NK.Admin_Auth	OE.NK.RNG	OE.AK.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.nhvs_Schutz	OE.AK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betrieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS	OE.NK.SW-Update
A.AK.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: Sämtliche Bedrohungen, organisatorische Sicherheitspolitiken und Annahmen, sowie die Sicherheitsziele wurden aus dem Protection Profile [77] übernommen. Entsprechend ist auch die Erklärung zu den Sicherheitszielen aus dem PP übernommen. Im PP werden dabei optionale Abbildungen von Sicherheitszielen auf Bedrohungen angegeben. Diese werden in Tabelle 4 des PPs als in Klammern gesetztes kleines Kreuz (x) dargestellt. In diesem ST wurden keine optionalen Beziehungen ausgewählt und die in Klammern gesetzten kleinen Kreuze (x) wurden aus der Tabelle entfernt. Es wurden keine Beziehungen ergänzt.

4.5.2. Überblick über die Sicherheitsziele des Anwendungskonnektors

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IED-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.SignaturVerifizier	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	**O.AK.VAU**	**O.AK.SGD**
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									x	x
T.AK.LAN.Admin		x																												
T.AK.Kanal_Missbrauch		x	x						x										x	x				x					x	x
T.AK.Mani.EVG					x													x			x	x	x							
T.AK.Mani.Client																					x	x				x				
T.AK.Mani.TI																					x	x								
T.AK.Mani.ExternerDienst																					x	x								
T.AK.Mani.Chipkarte																					x	x	x			x				
T.AK.Mani.Terminal																					x	x	x			x				
T.AK.Mani.AdminKonsole		x																			x	x								
T.AK.MissbrauchKarte																					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			x	
OSP.AK.Konn_Spez		x	x			x	x	x		x		x	x	x							x	x	x	x	x	x			x	x
OSP.AK.KryptAlgo	x																													

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IED-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.SignaturVerifizier	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	**O.AK.VAU**	**O.AK.SGD**
OSP.AK.SW-Update		x																			x	x	x							
OSP.AK.EVG_Modification					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																					x	x
OSP.AK.CardService				x		x																								
OSP.AK.Fachanwendungen																										x	x	x	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
T.AK.DTBS	x					x	x																x
T.AK.VAD	x					x	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
T.AK.LAN.eHKT	x																						
T.AK.LAN.CS																			x				
T.AK.WAN.TI															x								
T.AK.LAN.Admin																							
T.AK.Kanal_Missbrauch	x														x				x			x	
T.AK.Mani.EVG		x	x								x										x		
T.AK.Mani.Client											x								x				
T.AK.Mani.TI											x				x								
T.AK.Mani.ExternerDienst										x	x												
T.AK.Mani.Chipkarte						x	x	x	x	x	x											x	
T.AK.Mani.Terminal	x									x	x						x						
T.AK.Mani.AdminKonsole											x							x					
T.AK.MissbrauchKarte				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												
OSP.AK.KryptAlgo	x					x	x	x							x				x				
OSP.AK.SW-Update											x										x		
OSP.AK.EVG_Modification		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																							

	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
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							
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						
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. Abwehr der Bedrohungen durch die Sicherheitsziele

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.AK.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.

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.AK.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.AK.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.AK.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.AK.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 7) 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.

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.AK.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: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

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

Anwendungshinweis 74: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

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.AK.Protokoll, O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, O.NK.Schutz und OE.NK.KeyStorage 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.

Anwendungshinweis 75: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

T.NK.TimeSync

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

Anwendungshinweis 76: In diesem Security Target wurden keine optionalen Beziehungen zur Abwehr von Bedrohungen aus dem Protection Profile ausgewählt.

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[59]. 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

[59] 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.

erkanntem Angriff erfolgt ferner ein Eintrag mit Zeitstempel (O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro) in das Sicherheitsprotokoll (O.AK.Protokoll).

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

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.AK.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.PF_WAN, 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.AK.Basis_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.AK.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.

4.5.4. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

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

4.5.5. Detaillierte Erklärung für den Anwendungskonnektor

4.5.5.1. 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.

Im Fall der Kommunikation mit der VAU des ePA Aktensystems bzw. mit dem HSM des SGD wird die Bedrohung zusätzlich durch die Sicherheitsziele O.AK.VAU und O.AK.SGD abgewendet.

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. Im Fall der Kommunikation mit der VAU des ePA Aktensystems bzw. mit dem HSM des SGD wird die Bedrohung zusätzlich durch die Sicherheitsziele O.AK.VAU und O.AK.SGD abgewendet. 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 maipulierte 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.eGKevaluiert 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.

4.5.5.2. 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.Stapelsignatur, O.AK.Sig.Komfortsignatur und O.AK.Sig.SignQES fordern die Bereitstellung von Signaturdiensten für die Erstellung nicht-qualifizierter elektronischer Signaturen mit der SMC-B (s. OE.AK.SMC) und qualifizierter elektronische 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.VAU schützt den Datenaustausch zwsichen dem EVG und der VAU des ePA Aktensystems,
- 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 [92] und die Durchsetzung der zulässigen Signaturrichtlinien und Verschlüsselungsrichtlinien. Die EVG-Sicherheitsziele O.AK.Admin, O.AK.IFD-Komm (Kommunikation mit eHealth-Kartenterminals), O.AK.VAD, 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 [92] 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.

Die Sicherheitsziele O.AK.VAU und O.AK.SGD setzen Spezifikationsanteile von [92] um (und andere EVG-Sicherheitsziele präzisieren diese).

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 und O.AK.Sig.Stapelsignatur sowie O.AK.Sig.Komfortsignatur 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 nicht-qualifizierten 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.HBA und 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.Stapelsignatur und O.AK.Sig.Komfortsignatur 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.
- **O.AK.VAU** fordert die Ver- und Entschlüsselung von Daten im Rahmen der Kommunikation mit der VAU des ePA Aktensystems gemäß des spezifizierten VAU Protokolls.
- **O.AK.SGD** fordert die Ver- und Entschlüsselung von Daten im Rahmen der Kommunikation mit dem HSM des SGD gemäß des spezifizierten SGD Protokolls.
- 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 SicherheitszieleO.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. Das Sicherheitsziel O.AK.VAU verlangt den Schutz der Kommunikation zwischen dem EVG und der vertrauenswürdigen Ausführungsumgebung des ePA Aktensystems. Das Sicherheitsziel O.AK.SGD velangt den Schutz der Kommunikation zwischen dem EVG und dem HSM des Schlüsselgenerierungsdienstes (SGD). Die Anforderungen an die anderen Anteile der Fachanwendung werden durch das Umgebungsziel OE.AK.Fachdienste geeignet umgesetzt.

4.5.5.3. 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 der erweiterten Komponenten

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

Die Definition der Familie FPT_EMS wurde aus dem PP COS G2 [79], Abschnitt 6.6.1 übernommen.

Family **FPT_EMS – EVG Emanation**

Family behaviour This family defines requirements to mitigate intelligible emanations.

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

FPT_EMS.1 – EVG Emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit:FPT_EMS.1

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

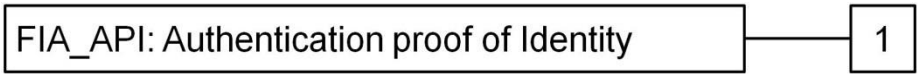
FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

5.2. Definition der Familie 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.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: FIA_API.1

There are no management activities foreseen

Audit: FIA_API.1

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. Hinweise und Definitionen

6.1.1. Hinweise zur Notation

Die Auswahl der funktionalen Sicherheitsanforderungen basiert auf der zum Zeitpunkt der Erstellung des Schutzprofils aktuellen Version 3.1 Revision 5 der Common Criteria; diese Version [2] liegt in englischer Sprache vor. Bereits in den zugrundeliegenden Schutzprofilen BSI-CC-PP-0097-V2 und BSI-CC-PP-0098-V3 wurden die Formulierungen an Common Criteria Version 3.1 Revision 5 in deutscher Sprache angepasst und in dem vorliegenden Security Target übernommen.

6.1.1.1. Sicherheitsziele des Netzkonnektors

Die Auswahl der funktionalen Sicherheitsanforderungen ist durch das zugrundeliegende Schutzprofil, BSI-CC-PP-0097-V2, gegeben. Das Schutzprofil basiert auf Version 3.1 Revision 5 der Common Criteria. Dieses Security Target basiert ebenfalls auf der aktuelleren Version 3.1 Revision 5 der Common Criteria und übernimmt die Formulierungen des Schutzprofils.

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 Verfeinerungen durch **fettgedruckten Text** in der Anforderung hervorgehoben und mit einer entsprechenden Fußnote gekennzeichnet oder sie werden der Anforderung in einem mit dem Wort „Refinement:“ eingeleiteten Absatz hinzugefügt. Gegebenenfalls werden sie in einem der Anforderung folgenden Anwendungshinweis näher erläutert. Gelöschter Text wird **~~fettgedruckt und durchgestrichen~~** dargestellt.

Die Operation **Auswahl** (selection) wird genutzt, um eine oder mehrere durch die CC vorgegebenen Optionen auszuwählen. In diesem Security Target wird eine bereits im PP ausgeführte Auswahl durch unterstrichenen Text in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben. Eine durch das PP bzw. CC Teil 2 [2] vorgegebene und im Security Target ausgeführte Auswahl wird zusätzlich durch [eckige Klammern] hervorgehoben.

Die Operation **Zuweisung** (assignment) wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Security Target werden bereits im PP ausgeführte Zuweisungen durch *kursiven Text* in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben. Durch das PP bzw. CC Teil 2 [2]vorgegebene und im Security Target ausgeführte Zuweisungen werden zusätzlich durch [*eckige Klammern*] hervorgehoben.

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.

6.1.1.2. Sicherheitsziele des Anwendungskonnektors

Die durchgeführten Operationen auf die funktionalen Sicherheitsanforderungen in Kapitel 6.2.7 sind wie folgt kenntlich gemacht:

Die Operation **Verfeinerung** wird genutzt, um Details zu einer Anforderung hinzuzufügen und schränkt diese Anforderung folglich weiter ein. In diesem Dokument werden Verfeinerung durch **fettgedruckten Text** in der Anforderung hervorgehoben und in einem der Anforderung folgenden Anwendungshinweis näher erläutert. Gelöschter Text wird ~~durchgestrichen~~ dargestellt.

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

Die Operation **Zuweisung** wird genutzt, um einem unspezifizierten Parameter einen spezifischen Wert zuzuweisen. In diesem Dokument werden Zuweisungen durch unterstrichenen Text in der Anforderung hervorgehoben und zusätzlich durch eine Fußnote der Originaltext angegeben. Führt die Operation der Zuweisung zu einer eingeschränkten Auswahl, die durch den Autor der Sicherheitsvorgaben (oder eines weiteren Schutzprofils) ausgeführt werden muss, ist dieser Text *unterstrichen und kursiv* gesetzt.

Die Operation **Iteration** wird genutzt, um eine Komponente mit unterschiedlichen Operationen zu wiederholen. In Dokument werden Iterationen durch einen Schrägstrich „/“ und den Iterationsidentifikator hinter dem Komponentenidentifikator angegeben.

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Das Schutzprofil BSI-CC-PP-0098-V3 betrachtet für jeden in Tabelle 7 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 7 definiert.

6.1.2.1. Subjekte

Subjekt	Beschreibung	Sicherheitsattribut
S_Administrator	Subjekt, das für einen Administrator handelt.	Siehe Tabelle 7.

Subjekt	Beschreibung	Sicherheitsattribut
S_Signaturdienst	Dienst des EVG zur Erstellung und Prüfung qualifizierter und nichtqualifizierter elektronischer Signaturen	Das Subjekt übernimmt die Sicherheitsattribute des aufrufenden Benutzers
S_Verschlüsselungs-dienst	Dienst des EVG zur Verschlüsselung und Entschlüsselung von Dokumenten	Kein Sicherheitsattribut
S_Chipkartendienst	Dienst des EVG zur Verwaltung und zum Zugriff auf gesteckte Chipkarten	Kein Sicherheitsattribut
S_Kartenterminal-dienst	Dienst des EVG zur Verwaltung und zum Zugriff auf eHealth-Kartenterminals	Kein Sicherheitsattribut
S_TSL_Dienst	Zentraler TSL-Dienst der TI nach [104]. 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
S_AK	Subjekt, das für einen Prozess des AK handelt, der für einen Funktionsaufruf des Clientsystems oder eines Fachmoduls handelt.	Aufrufender: Das Sicherheitsattribut 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.	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.

Subjekt	Beschreibung	Sicherheitsattribut
		Kartenslot: Adresse des Kartenslots und die darin gesteckte Chipkarte. Authentisierungsstatus: - „nicht identifiziert“ – Kartenterminal unbekannter 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 Entschlüsselungsschlüsselinhabers für verschlüsselte Daten.[60] 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, - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten - eindeutige Referenz des Entschlüsselungsschlüsselinhabers für verschlüsselte Daten.[61]

[60] 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.

[61] 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
		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
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

Subjekt	Beschreibung	Sicherheitsattribut
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“.
S_Verzeichnisdienst (VZD)	Zentraler Verzeichnisdienst (VZD) in der TI nach [105]. 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.
S_ePA_Fachmodul	Subjekt des ePA Fachmodules	Identität: eindeutiger Name zur Identifizierung des Fachmoduls

Tabelle 14: Subjekte

6.1.2.2. Objekte

Das Schutzprofil BSI-CC-PP-0098-V3 betrachtet 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.
Logischer Kanal einer Chipkarte	Logischer Kanal eines HBA, einer SMC oder einer eGK.	Sicherheitszustand: Sicherheitszustand des logischen Kanals der Chipkarte (vergl. COS-Spezifikation [97]).
SICCT-Kommando	Kommandos zur Steuerung der eHealth-Kartenterminals. Die SICCT-Kommandos dienen [94] [96] - der Steuerung des eHealth-Kartenterminals, insbesondere zur Kommunikation mit dem Konnektor, Kommandoabarbeitung und Konfiguration der eHealth-	Typ des SICCT-Kommandos: - eHKT-Steuerungskommando, - Benutzerkommuikationskommando, - Chipkartenkommando, - PIN-Prozesskommando.

Objekt	Beschreibung	Sicherheitsattribut
	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 „Benutzerkommuikationskommando“ 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).	
Antwort auf SICCT-Kommando	Antwortnachricht des eHealth-Kartenterminals auf ein zuvor gesendetes SICCT-Kommando, siehe [96].	Kein 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[62].	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	Kein Sicherheitsattribut

[62] 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
	Signaturschlüsselinhabers mit der Signatur-PIN gegenüber der Signaturchipkarte) durch den Signatur-dienst an die Signaturkarte zum Signieren gesendet wird.	
Signierte Dokumente	Daten, denen eine digitale Signatur zugeordnet ist. Die Vertraulichkeit signierter Daten ist zu schützen[63]. Die signierten Daten dürfen durch den EVG nicht verändert werden.	Signaturrichtlinie: Beschreibung der Regeln, wie die Daten zu prüfen sind. 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. Die Vertraulichkeit und Integrität des Prüfergebnisses ist zu schützen[64].	Kein Sicherheitsattribut
Zu signierender Bitstring	Bitstring von maximal 512 Bit die dem EVG zur Weitergabe and Chipkarten und Erzeugung digitaler Signaturen zum Zweck der Authentisierung von	Kein Sicherheitsattribut

[63] 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.

[64] Der Schutz der Vertraulichkeit der Prüfungsergebnisse ergibt sich hier aus dem Bezug zu den vertraulichen zu signierenden bzw. signierten Daten.

Objekt	Beschreibung	Sicherheitsattribut
	Benutzern gegenüber anderen Instanzen übergeben werden.	
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 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

Objekt	Beschreibung	Sicherheitsattribut
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 innerhalb der Kontrolle des EVG zu gewährleisten.	Kein Sicherheitsattribut
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 [98],	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 and den Konnektor[65]	Kein Sicherheitsattribut
Authentisierungs-verifikationsdaten (VAD)	Datum, das vom Benutzer zum Nachweis seiner Identität gegenüber Chipkarten dient. Dies sind VAD der Kartenhalter und die SVAD[66] 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-Terminal eingegeben und an die Chipkarte übergeben. Dieses Datum kann eine PIN oder eine PUK sein[67]. Die Vertraulichkeit und Integrität[68] der VAD müssen geschützt werden.	Kein Sicherheitsattribut

[65] 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.

[66] Englisch: signatory verification authentication data.

[67] Der Heilberufsausweis als qualifizierte Signaturerstellungseinheit unterstützt nur die Authentisierung durch Wissen.

[68] Der Schutz der Integrität ist insbesondere bei einem Wechsel der SVAD erforderlich.

Objekt	Beschreibung	Sicherheitsattribut
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[69] 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 empfangenen Daten werden entschlüsselt und integritätsgeprüft. Es werden unverfälscht empfangene Daten ausgegeben.	Kein Sicherheitsattribut
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:

[69] 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
		• 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 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
Mandant	Nach dem Informationsmodell werden Mandanten dem Clientsystem sowie vom	Kein Sicherheitsattribut

Objekt	Beschreibung	Sicherheitsattribut
	Konnektor verwalteten externen Ressourcen (Kartentermi-nal mit Slots, Arbeitsplatz mit Signaturproxy und SMC-Bs) persistent zugeordenet .	
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. [92], 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 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
Response SGD-HSM	Antwort eines SGD-HSM auf eine Anfrage durch S_ePA_Fachmodul.	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 22 nach den jeweiligen Komponenten FDP_ACF definiert, bei FDP_ACF.1/SGD erfolgt die Beschriebung direkt im SFR.

6.1.2.3. TSF Daten

TSF Datum	Beschreibung
Öffentlicher Schlüssel zur Prüfung der 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 der 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 Verschlüsselungszertifikate (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.
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.

TSF Datum	Beschreibung
Arbeitsplatz-konfigurationsdaten	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 1.3.5.1 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

(1) VPN-Client: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);

(2) Dynamischer Paketfilter: sowohl für WAN als auch für LAN;

(3) Netzdienste: Zeitsynchronisation über sicheren Kanal, Zertifikatsprüfung mittels Sperrlisten;

(4) Stateful Packet Inspection: Generierung von Audit-Daten für spätere zustandsgesteuerte Filterung;

(5) Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, optional sichere Kanäle zu anderen Komponenten des Konnektors, Protokollierung Sicherheits-Log;

(6) Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, eingeschränkte Möglichkeit der Administration von Firewall-Regeln;

(7) 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 des Netzkonnektors aus diesem Kapitel wurde zudem das Suffix „NK“ verwendet, selbst wenn keine Iteration vorliegt.

6.2.1. VPN-Client

VPN

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

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

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_TI The TSF shall provide a communication channel between itself and another trusted IT product **VPN-Konzentrator der Telematikinfrastruktur**[70] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[71] and protection of the channel data from modification **and**[72] disclosure.

FTP_ITC.1.2/NK.VPN_TI The TSF shall permit the TSF[73] 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*[74].

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 [92], RFC 4301 (IPsec) [49], RFC 4303 (ESP) [52]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [53]) 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).

70 refinement

71 refinement

72 refinement (or → and)

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

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

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)**[75] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[76] and protection of the channel data from modification **and**[77] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[78] 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*[79].

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 [92], RFC 4301 (IPsec) [49], RFC 4303 (ESP) [52]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [53]) 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).

75 refinement

76 refinement

77 refinement (or → and)

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

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

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) [53], siehe [87], 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: Eine theoretisch mögliche Kommunikation von EVGs untereinander wird in diesem Security Target nicht behandelt.

Informationsflusskontrolle

Die Informationsflusskontrolle ergibt sich zwar aus der Betrachtung der VPN-Kanäle (aufgrund der Frage: Wie wird der Eingang in den VPN-Tunnel geschützt?), sie wird aber im Hinblick auf ihre Realisierung der Anforderung nach Informationsflusskontrolle mittels einem dynamischen Paketfilter (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF) zugeordnet; das „PF“ steht dabei für Paketfilter. Daher finden sich die Anforderungen (SFR) zu diesen Aspekten im nächsten Abschnitt.

Die von O.NK.PF_WAN und O.NK.PF_LAN erzwungene VPN-Nutzung für zu schützende Daten der TI und der Bestandsnetze und für *zu schützende Nutzerdaten* (im Sinne des Abschnitts 3.1) wird durch FDP_IFF.1.2/NK.PF umgesetzt, sofern die Paketfilter-Regeln geeignet gesetzt sind, was wiederum durch die Administratordokumentation (siehe das Refinement zu AGD_OPE.1 in Abschnitt 6.4) sichergestellt wird.

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Alle funktionalen Anforderungen, die mit dem Paketfilter in direktem Zusammenhang stehen, wurden mit dem Suffix „/NK.PF“ (wie Paketfilter) versehen.

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)*[80] on the *subjects*

80 [assignment: *information flow control SFP*]

(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) hash&URL server,

(10) registration server of the VPN network provider,

(11) remote management server,

the information

- *incoming information flows*
- *outgoing information flows*

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[81].

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.

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

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der LAN-Adapter des Konnektors angeschlossen ist.
ANLW_LEKTR_INTRANET_ROUTES	Adressbereich des Intranet-VPN des LE
NET_SIS	VPN-Konzentratoren der SIS
NET_TI_ZENTRAL	Zentrale Dienste der TI
NET_TI_DEZENTRAL	Adressbereich der WAN-Schnittstellen der Konnektoren für die Kommunikation mit der TI oder den Bestandsnetzen
NET_TI_OFFENE_FD	Offene Fachdienste der TI
NET_TI_GESICHERTE_FD	Gesicherte Fachdienste der TI
ANLW_BESTANDSNETZE	die an die TI angeschlossenen Bestandsnetze
ANLW_AKTIVE_BESTANDSNETZE	die an die TI angeschlossenen und vom Administrator freigeschalteten Bestandsnetze
VPN_KONZENTRATOR_TI_IP_ADDRESS	IP-Adresse des VPN-Konzentrators der TI
VPN_KONZENTRATOR_SIS_IP_ADDRESS	IP-Adresse des VPN-Konzentrators des SIS
DNS_SERVERS_BESTANDSNETZE	IP-Adressen von DNS-Servern für die Bestandsnetze (ANLW_BESTANDSNETZE)
CERT_CRL_DOWNLOAD_ADDRESS	IP-Adresse des CRL-Download-Servers
DNS_ROOT_ANCHOR_URL	IP-Adresse des DNSSEC Vertrauensankers für das Internet
hash&URL-Server	IP-Adresse des hash&URL-Servers
registration server	IP-Adresse des Registrierungsservers
remote management server	IP-Adresse des Remote-Managementservers
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.
TSL_DOWNLOAD_ADDRESS	IP-Adresse des TSL-Download-Punktes des TSL-Dienstes.

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*[82] 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:

- *IP address,*
- *port number,*
- *protocol type,*
- *direction (inbound and outbound IP*[83] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES. [84]

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

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

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

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

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

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

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

82 [assignment: *information flow control SFP*]

83 IP = Internet Protocol

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

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

d. by means of protocol HTTP with IP-Address TSL_DOWNLOAD_ADDRESS,

e. 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≠““).[85]

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

(14) The TSF shall enforce SFP rules ANLW_FW_SIS_ADMIN_RULES

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

(15) *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*[86].

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*][87].

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.

(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.

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

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

(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*][88].

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 erbracht.

Der Mechanismus „Logische Trennung“ (siehe [gemSpec_Kon], TIP1-A_4823) wird vom RISE Konnektor nicht implementiert. Für das Attribut MGM_LOGICAL_SEPARATION kann der Wert daher nicht auf ENABLED gesetzt werden.

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

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 6.4) 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 (kurze) Historie der Verbindung durch die Funktionalität des Betriebsystemkernels. Eingehende Verbindungen werden nur als Antworten auf zuvor ausgegangene Anfragen zugelassen, so dass ein ungefragter Verbindungsaufbau aus dem WAN wirkungsvoll verhindert wird.

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] [106], Tabelle 1 aufgeführten Protokolle zulässig. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.
Entsprechend der Anforderungen an die in O.NK.PF_LAN beschriebene Informationsflusskontrolle, erzwingt der EVG, 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 ergänzt.

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*[89] to provide restrictive[90] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [*administrators* (*local administrator, super administrator)*] to specify alternative initial values to override the default values when an object or information is created.

Refinement: Bei den Sicherheitsattributen handelt es sich um die Filterregeln für den dynamischen Paketfilter (FDP_IFF.1.2/NK.PF). *Restriktive* bedeutet, dass Verbindungen, die nicht ausdrücklich erlaubt sind, automatisch verboten sind. Außerdem muss der EVG bei

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

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

Auslieferung mit einem Regelsatz ausgeliefert werden, der bereits einen grundlegenden Schutz bietet.

Anwendungshinweis 84: Der Netzkonnektor unterscheidet intern zwischen den Rollen local administrator und super administrator. Alle administrativen Rollen können alternative Default-Werte im Sinne von FMT_MSA.3/NK.PF spezifizieren.

Erläuterung: FMT_MSA.3/NK.PF erfüllt die Abhängigkeit von FDP_IFF.1/NK.PF, weil es die Festlegung von Voreinstellungen für die Paketfilter-Regeln fordert und klärt, welche Rollen die Voreinstellungen ändern können. Die hier noch nicht erfüllten Abhängigkeiten (FMT_MSA.1/NK.PF und FMT_SMR.1./NK) werden in Abschnitt 6.2.4 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.AK.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.AK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [48] erreicht.

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

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

Anwendungshinweis 85: Zum Zeitdienst siehe Konnektor-Spezifikation [92], Abschnitt 4.2.5 Zeitdienst.

Anwendungshinweis 86: Die im Refinement angegebene Zeitsynchronisation entspricht den Anforderungen der Konnektor-Spezifikation [92] (einmal innerhalb von 24 Stunden).
Gemäß Konnektor-Spezifikation [92], Abschnitt 3.3 Betriebszustand, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [92] „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, die den Betriebszustand (Power, Verbindungsstatus, Fehlerzustand) am Konnektorgehäuse anzeigen, um die benannte Anforderung der Spezifikation umzusetzen, siehe LS14 und PS4 in Kapitel 1.3.3. Der NK meldet bei einer nicht erfolgten Zeitsynchronisation dem AK den Fehlerzustand, so dass dieser via Ereignisdienst seine Benutzer informieren kann. Zusätzlich wird an der Signaleinrichtung der kritische Betriebszustand angezeigt.

Anwendungshinweis 87: Gemäß Konnektor-Spezifikation [92], Abschnitt 3.3 *Betriebszustand*, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [92]: *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 besitzt eine Signaleinrichtung in Form von Status-LEDs, welche den Betriebszustand am Gehäuse des Konnektors anzeigt, um die benannte Anforderung der Spezifikation umzusetzen, siehe LS14 und PS4 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*[91] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[92] when interpreting the TSF data from another trusted IT product.

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

92 [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 der Konnektor-Spezifikation [92]. Der Konnektor prüft insbesondere auch die Integrität der TSL; die Modellierung mit SFRs aus der Familie FCS_COP erfolgt jedoch gemäß [78] im Teil Anwendungskonnektor (XML-Signaturprüfung).
Darüber hinaus muss der Konnektor die für den Download der Hash-Datei der TSL(ECC-RSA) genutzte Verbindung zum TSL-Dienst durch TLS absichern und die Anforderungen aus A_17661 [93] umsetzen.

Anwendungshinweis 89: Die TSL und die CRL muss gemäß Anforderung A_4684 in der Konnektor-Spezifikation [92] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden.
Der Konnektor kann die TSL und die CRL bei Bedarf manuell importieren (siehe Anforderung TIP1-A_4705 und TIP1-A_4706 in [93]).
Im Rahmen der ECC-Migration muss der Konnektor bei der Initialisierung des neuen Vertrauensankers (ECC-RSA) Cross-Zertifikate verwenden (vgl. A_17837-01 und A_17821) und das TSL-Signer-CA-Zertifikat (ECDSA) als TI-Vertrauensanker und die TSL(ECC-RSA) verwenden (A_17688). Zur Signaturprüfung der TSL müssen die Vorgaben aus A_17205 und A_21185 berücksichtigt werden. Der EVG muss den neuen TI-Vertrauensanker im sicheren Datenspeicher speichern (gem. A_17548 [93]).
Im Rahmen der Aktualisierung der TSL werden die Vorgaben aus TIP1-A_4693-02 in [93] umgesetzt werden. Dabei wird sichergestellt, dass, abweichend von anderen Fällen, in denen lediglich die eingebettete XML-Signatur geprüft werden, bei einem TSL Download aus dem Internet die detached signature vom Konnektor heruntergeladen und geprüfen wird.

6.2.4. Stateful Packet Inspection

Anwendungshinweis 90: Weitergehende Angriffe gegen die Systemintegrität des EVG werden abgewehrt (robuste Implementierung, Resistenz gegen Angriffe wie von der Vertrauenswürdigkeitskomponente der Klasse AVA_VAN laut Abschnitt 0 gefordert), aber nicht im Detail erkannt, d.h. es eine komplexe Erkennungslogik ist weder gefordert noch implementiert.

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

6.2.5. Selbstschutz

Speicheraufbereitung

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[93] the following objects: *cryptographic keys (and session keys) used for the VPN or for TLS-connections, user data (zu schützende Daten der TI und der* Bestandsnetze *and zu schützende Nutzerdaten)*, [*none*][94].

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 Konnektor speichert zu schützende Daten der TI und der Bestandsnetze oder zu schützende Nutzerdaten niemals dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z. B. während einer Ver- oder Entschlüsselung).

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][95] to demonstrate the correct operation of [the TSF][96].

FPT_TST.1.2/NK The TSF shall provide authorised users with the capability to verify the integrity of TSF data[97].

FPT_TST.1.3/NK The TSF shall provide authorised users with the capability to verify the integrity of [TSF][98] .

Refinement: Zur Erfüllung der Anforderungen aus FPT_TST.1/NK muss der EVG mindestens die Mechanismen implementieren, welche dem aktuellen Stand der Technik bei Einzelplatz-Signaturanwendungen entsprechen. Dazu gehören insbesondere:

a) die Prüfung kryptographischer Verfahren bei Programmstart,

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

94 [assignment: *list of objects*]

95 [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*]]

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

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

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

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

Anwendungshinweis 92: Die kryptographischen Verfahren werden in Software implementiert. Der Benutzer kann die self tests durch Neustart des EVGs selbst anstoßen. Die im Refinement geforderten Mechanismen werden wie folgt umgesetzt:

- Eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (z. B. Konfigurationsdateien, TSF-Daten) mit kryptographischen Verfahren beim Programmstart
- Der EVG nutzt den physikalischen Zufallszahlengenerator der gSMC-K (OE.NK.RNG) als Seed Quelle für den Zufallszahlengenerator des Betriebssystems. Es werden keine weiteren physikalischen Zufallszahlengeneratoren verwendet.

Schutz von Geheimnissen, Seitenkanalresistenz

Zur Definition der Anforderung FPT_EMS.1/NK siehe Abschnitt 5.1.

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)*[99] in excess of *limits that ensure that no leakage of this sensitive data occurs*[100] enabling access to

- *session keys derived in course of the Diffie-Hellman-Keyexchange-Protocol,*
- *[none]*[101],
- *[none]*[102],
- *[none]*[103],

99 [assignment: *types of emissions*]

100 [assignment: *specified limits*]

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

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

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

- *[key material used for authentication of administrative users]*[104],
- *[passwords used for authentication of administrative users]*[105] and
- *data to be protected ("*zu schützende Daten der TI und der Bestandsnetze")
- *[none]*[106].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)*[107] are unable to use the following interface *WAN interface or LAN interface of the connector*[108] to gain access to **the sensitive data (TSF data and user data) listed above**[109].

Anwendungshinweis 93: Es wurden keine weiteren Verfeinerungen vorgenommen. Die Integritätsprüfung bei Selbsttest und Software-Update erfolgt anhand von öffentlichen Signatur-Schlüsseln. Die Software Images werden über einen sicheren Kanal (VPN/TLS) übertragen. Die Images selbst sind dabei unverschlüsselt. Für die entsprechenden Auswahl Operationen des PPs [77] wurde daher „none" gewählt. Die Authentisierung des Administrators wird vom Netzkonnektor durchgeführt. Dieser schützt die Authentisierungsschlüssel und Passwörter vor Offenlegung.

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][110] level of audit; and

c)

- *start-up, shut down and reset (if applicable) of the TOE*

104 *[selection: none, key material used for authentication of administrative users (if applicable)]*

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

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

107 [assignment: *type of users*]

108 [assignment: *type of connection*]

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

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

- *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.*[111]
- *operational states according to [92], table 3*[112]

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

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*][113].

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.

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

112 refinement

113 [assignment: *other audit relevant information*]

Anwendungshinweis 94: Es werden alle in der Konnektor-Spezifikation [92] (Abschnitte 3.2 und 3.3, Tabelle 3) aufgeführten Fehlerzustände 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; dieser Zeitpunkt wird als Zeitpunkt für das Ereignis „start up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet. Analog wird der Protokollierungsdienst als letzter Dienst bei einem shut-down des EVG beendet und ensprechend als Zeitpunkt für das Ereignis „shut down“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet.

Anwendungshinweis 95: Der Netzkonnektor muss auf einer HW betrieben werden, die ausreichend Speicherplatz für die Log-Einträge zur Verfügung stellt, siehe Kapitel 1.3.6. Zusätzlich implementiert der Netzkonnktor die folgenden Mechanismen um die sichere Protokollierung von Ereignissen zu gewährleisten: Zusammenfassung aufeinanderfolgender Einträge gleicher Ereignisse mit Angabe der Anzahl, Log Rotation und Komprimierung archivierter Logs.

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 authentisierte Administratoren (username, password) die Identität des ändernden Administrators (username) und die die jeweilige Administrator-Rolle in das Sicherheits-Log auf.

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* **(*local administrator, super administrator)***[114],
- *SIS,*
- *TI*
- *Anwendungskonnektor*[115].

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

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

Anwendungshinweis 97: Der EVG unterstützt die Rolle Administrator.

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/AK. Die Rollen SIS und TI werden nur im Zusammenhang mit den Paketfilterregeln für die Kommunikation mit deren VPN-Konzentratoren verwendet.

FMT_MTD.1/NK Management of TSF data

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

FMT_MTD.1.1/NK The TSF shall restrict the ability to [query, modify, delete, clear, [*activate/deactivate (VPN connection)*]][116] the *real time clock, packet filtering rules [VPN connection]*[117] to *the role Administrator*[118].

Refinement: Die *real time clock* bezieht sich auf die von OE.AK.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

114 refinement

115 [assignment: *the authorised identified roles*]

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

117 [assignment: *list of TSF data*]

118 [assignment: *the authorised identified roles*]

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. Die Operationen *query* und *modify* sind auf die *real time clock* anwendbar. Die Operationen *query, modify, delete* und *clear* können auf die *packet filtering rules* angewended werden. Für die *VPN connection* sind nur die Operationen *activate* und *deactivate* zulässig.

Anwendungshinweis 100: Nur der Administrator kann das Deaktivieren der VPN-Verbindung vornehmen. Die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ wurde in die Liste bei FMT_SMF.1/NK aufgenommen. Innerhalb von FMT_MTD.1/NK wird der Zugriff auf diese Managementfunktion auf den Administrator beschränken.

FIA_UID.1/NK.SMR Timing of identification

Identification of Security Management Roles

Dependencies: No dependencies.

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

- *all actions except for administrative actions (as specified by FMT_SMF.1*/NK*, see below)*[119]

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) wird in diesem Security Target nicht weiter eingeschränkt. Vor administrativen Tätigkeiten ist die Identifikation verpflichtend.

FTP_TRP.1/NK.Admin Trusted path

Trusted Path für den Administrator.

Dependencies: No dependencies.

FTP_TRP.1.1/NK.Admin The TSF shall provide a communication path between itself and [*local*] users that is logically distinct from other communication paths and provides assured identification of its end

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

points and protection of the communicated data from [modification, disclosure][120]

FTP_TRP.1.2/NK.Admin The TSF shall permit [the TSF, local users][121] 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*.[122]

Anwendungshinweis 102: Die Wartung kann nur über die LAN-Schnittstelle (PS1) erfolgen.

FMT_SMF.1/NK Specification of Management Functions

Dependencies: No dependencies.

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

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

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

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.) [123]

- *Aktivieren und Deaktivieren des VPN-Tunnels*[124]

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

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

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

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

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

124 refinement: **Aktivieren und Deaktivieren des VPN-Tunnels**

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*[125] to restrict the ability to *[query, modify, delete]*[126] the security attributes *packet filtering rules*[127] to *the roles „Administrator“, [no other authorised identified roles]*[128].

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

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

betreffen, dürfen nicht über die Administrator-Schnittstelle verändert werden können. Der Administrator muss den gesamten WAN-seitigen Verkehr blockieren können (siehe Konnektorspezifikation [92], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [92], 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

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

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

127 [assignment: *list of security attributes*]

128 [assignment: *the authorised identified roles*]

angesehen) nur durch den Administrator oder eine andere kompetente Instanz (siehe FMT_SMR.1./NK) verändert werden können. Weiterhin legt die Konnektorspezifikation [92] 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: Unter *„Administrator"* werden hier alle Administrator-Rollen verstanden (local, super). Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [92] definierten Anforderungen.

Anwendungshinweis 105: Firewall-Regeln, die nicht durch den Administrator angepasst werden dürfen, können durch das Einspielen eines Software-Updates aktualisiert werden.

Anwendungshinweis 106: Der Netzkonnektor kann seine Filterregeln abhängig von Ereignissen anderer Konnektorteile (z. B. Anwendungskonnektor) dynamisch anpassen.

FMT_MSA.4/NK Security attribute value inheritance

Definition von Regeln für die Sicherheitsattribute

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

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

Die Authentisierung des Administrators ***~~kann gemäß OE.NK.Admin_Auth in der IT-Einsatzumgebung erfolgen~~ wird durch den Netzkonnektor selbst durchgeführt*** [129]

129 refinement

Wenn die Authentisierung des Administrators ~~***in der IT-Einsatzumgebung erfolgt und***~~[130] *erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diese Autorisierung und weisen dem Sicherheitsattribut „Autorisierungsstatus" des auf diese Weise authentisierten Benutzers „Administrator" den Wert „****autorisiert****" zu.*

Wenn die Authentisierung des Administrators ~~***in der IT-Einsatzumgebung erfolgt und***~~[131] *nicht erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diesen Status und weisen dem Sicherheitsattribut „Autorisierungsstatus" des auf diese Weise nicht authentisierten Benutzers „Administrator" den Wert „****nicht autorisiert****" zu.*[132]

Subjekt	Sicherheitsattribut	Mögliche Werte
Administrator	Autorisierungsstatus	autorisiert, nicht autorisiert

Anwendungshinweis 107: Die Authentisierung des Administrators erfolgt gemäß O.NK.Admin_Auth durch den Netzkonnektor selbst. OE.NK.Admin_Auth wird daher als automatisch erfüllt betrachtet.

Software Update

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

Zugriffskontrolle – Updates

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*][133] on

[*subjects:*

(1) Administrator (S_Administrator),

132 [assignment: *rules for setting the values of security attributes*] (die Schriftauszeichnungen im Zuweisungstext dienen (wenn nicht explizit durch Fussnoten gekennzeichnet) der besseren Leserlichkeit und kennzeichnen hier keine ausgeführten Operationen)

132 [assignment: *rules for setting the values of security attributes*] (die Schriftauszeichnungen im Zuweisungstext dienen (wenn nicht explizit durch Fussnoten gekennzeichnet) der besseren Leserlichkeit und kennzeichnen hier keine ausgeführten Operationen)

132 [assignment: *rules for setting the values of security attributes*] (die Schriftauszeichnungen im Zuweisungstext dienen (wenn nicht explizit durch Fussnoten gekennzeichnet) der besseren Leserlichkeit und kennzeichnen hier keine ausgeführten Operationen)

133 [assignment: *access control SFP*]

(2) Anwendungskonnektor (S_AK),

(3) Netzkonnektor (S_NK);

objects:

(1)Update-Pakete

operations:

(1) Importieren

(2) Verwenden][134]

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.

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

Sicherheitsattribute für Zugriffskontrolle – Updates.

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

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

135 [assignment: *access control SFP*]

[*subjects:*

(1) S_Administrator,

(2) S_AK,

(3) S_NK,

objects:

(1)Update-Pakete with security attributes:

a) Signatur,

b) Zulässige Software-Versionen

]136

FDP_ACF.1.2/NK.Update The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

(1) Das Subjekt S_AK oder S_NK 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.

]137

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*]138.

FDP_ACF.1.4/NK.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.

136 [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*]

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

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

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

]¹³⁹

Anmerkung: Die Integrität und Authentizität der Update-Dateien wird durch die Verifikation von kryptografischen Signaturen geprüft. Dabei werden Signaturen nach RSASSA-PKCS1-v1_5 with SHA256 (siehe [31]) und 2048 Bit Schlüssellänge verwendet. Die XML-Dateien UpdateInfo.xml und FirmwareGroupInfo.xml werden durch Signaturen nach RSASSA-PSS with SHA256 (siehe [31]) und 2048 Bit Schlüssellänge geschützt.

Hinweis: Die Liste der zulässigen Software-Versionen wird in der Spezifikation Einführung der Gesundheitskarte. Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM] mit “Firmware-Gruppe” bezeichnet [103]. Diese muss als versionierte Liste zulässiger Firmware-Versionen für Software-Updates in jede Konnektor-Software integriert werden.

FTP_ITC.1/NK.KSR Inter-TSF trusted channel / Zum KSR (Update-Server)

Import von Update-Paketen.

Dependencies: No dependencies

Hierarchical to: No other components

FTP_ITC.1.1/NK.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/NK.KSR The TSF shall permit the TSF[140] to initiate communication via the trusted channel

FTP_ITC.1.3/NK.KSR The TSF shall initiate communication via the trusted channel for Prüfung auf neue Firmware-Update-Pakete und Download neuer Firmware-Update-Pakete[141].

Hinweis: Die Verfeinerung des Elementes FTP_ITC.1/NK.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.

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

140 [selection: the TSF, another trusted IT product]

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

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

Integrität von Update-Paketen.

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: FTP_ITC.1/AK.KSR

FDP_UIT.1.1/NK.Update The TSF shall enforce the [*Update-SFP*][142] to [receive][143] user data ~~**in a manner**~~[144] protected from [modification, deletion, insertion][145] errors.

FDP_UIT.1.2/NK.Update The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion][146] has occurred.

6.2.7. Kryptographische Basisdienste

Anwendungshinweis 108: Die SFR der Familie FCS in CC Teil 2 [2] enthalten ein [assignment: cryptographic algorithm]. Diese Zuweisungen wurden durch das PP [77] in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI vorgenommen. Die TSF implementieren die darüberhinausgehenden verpflichtenden Vorgaben der angegebenen Standards soweit sie die angegebenen Algorithmen und Protokollen betreffen; es wird dabei 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 [*86*] 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.

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

143 [selection: *transmit, receive*]

144 refinement

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

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

Anwendungshinweis 109: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Die AES Implementierung des EVGs verwendet keine zusätztlichen HW Mechanismen (AES-NI) zur Berechnung der AES-Verschlüsselungen und -Entschlüsselung.

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*[147] in accordance with a specified cryptographic algorithm *SHA-1, SHA-256, [none]*[148] and cryptographic key sizes *none*[149] that meet the following: *FIPS PUB 180-4 [14]*.[150]

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

147 [assignment: *list of cryptographic operations*]

148 *[assignment: list of SHA-2 Algorithms with more than 256 bit size]*

149 [assignment: *cryptographic key sizes*]

FCS_COP.1.1/NK.HMAC The TSF shall perform *HMAC value generation and verification*[151] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, [SHA-256]*[152] and cryptographic key sizes [*128 bit and 256 bit*][153] that meet the following: *FIPS PUB 180-4 [14], RFC 2404 [56], RFC 4868 [57], RFC 7296 [53]*.

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 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

- *verification of digital signatures and*
- *signature creation with support of gSMC-K storing the signing key and performing the RSA operation* [154]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[155] and cryptographic key sizes *2048 bit*[156] that meet the following: *RFC 8017 (RSASSA-PKCS1-v1_5) [31], FIPS PUB 180-4 [14]*.

---

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

[152] *[assignment: list of SHA-2 Algorithms with 256bit size or more]*

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

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

[155] [assignment: *cryptographic algorithm*]

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

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*[157] in accordance with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42)*[158] and cryptographic key sizes *256 bit*[159] that meet the following: *FIPS 197 [15], RFC 3602 [55], RFC 4303 (ESP) [52],], specification [86]* [160].

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*[161] in accordance with a specified cryptographic algorithm *IPsec-*

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

[158] [assignment: *cryptographic algorithm*]

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

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

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

protocol[162] and cryptographic key sizes *256 bit*[163] that meet the following: *RFC 4301 (IPsec) [49], specification [86]*[164].

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 [*PRF_HMAC_SHA1 and PRF_HMAC_SHA256*][165] and specified cryptographic key sizes [*128 bit and 256 bit*][166] that meet the following: *RFC 2104 [18], RFC 7296 [53], specification [86], TR-03116 [76]*[167].

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 [2] entweder durch eine Schlüsselgenerierung (FCS_CKM.1) oder durch einen Schlüsselimport (FDP_ITC.1 oder FDP_ITC.2) zu erfüllen sind. In diesem Security Target wurde (entsprechend zum PP) eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols seine Sitzungsschlüssel (session keys) für die VPN-Kanäle ableitet; diese Ableitung wird als Schlüsselgenerierung angesehen. (Der Aspekt des Schlüsselaustausches mit einem VPN-Konzentrator wird als FCS_CKM.2/NK.IKE modelliert, siehe unten). Alle erzeugten Schlüssel besitzen mindestens 100 Bit Entropie, damit der EVG resistent gegen Angriffe mit hohem Angriffspotential sein kann.

[162] [assignment: *cryptographic algorithm*]

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

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

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

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

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*[168] that meets the following *standard: RFC 7296 [53], specifications [86], TR-02102-3 [73]*[169].

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 [*overwriting with fixed bit pattern*][170] that meets the following: [*none*][171].

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 6.2.6 für TLS-Kanäle verwendeten Schlüssel. Die Schlüssel werden durch das überschreiben mit Nullen oder festen Werten zerstört.

168 [assignment: *cryptographic key distribution method*]

169 [assignment: *list of standards*]

170 [assignment: *cryptographic key destruction method*]

171 [assignment: *list of standards*]

Anwendungshinweis 112: Die Operationen stehen im Einklang mit den in Dokumenten [76], [*86*] und [92] angegebenen Vorgaben. Dies gilt insbesondere für alle genannten SFRs FCS_COP.1/* sowie FCS_CKM.1/NK, FCS_CKM.2/NK.IKE und FCS_CKM.4/NK. Gleiches gilt für die in Kapitel 6.2.6 für TLS-Kanäle definierten Kryptoverfahren.
Der DH-Exponent für den Schlüsselaustausch hat eine Mindestlänge gemäß [*86*]. Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy wurden die Vorgaben aus [*86*] beachtet.

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

Hinweis 1: Tatsächlich verwendet werden die von der Spezifikation geforderten TLS-Verbindungen erst im Anwendungskonnektor.

Hinweis 2: TLS-Verbindungen werden auch für die Absicherung einer Administrationsschnittstelle des Netzkonnektors verwendet. Die SFRs in diesem Kapitel werden dafür mit genutzt und wurden 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[172] provides assured identification of its end points and protection of the channel data from modification and[173] disclosure.

FTP_ITC.1.2/NK.TLS The TSF must be able to[174] permit *the TSF or another trusted IT-Product*[175] 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, [administration]*[176].

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

172 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.

173 refinement (or → and)

174 refinement (shall → must be able to)

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

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

„integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von unbefugtem Löschen, Einfügen oder Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss auf Basis des TLS-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [93] und [*86*], wobei TLS 1.2 gemäß RFC 5246 [59] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,

TLS_DHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch und bei der Signaturprüfung mittels ECDSA MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Daneben SOLLEN die Kurven brainpoolP256r1 und, brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt und verwendet werden. Andere Kurven SOLLEN NICHT verwendet werden, damit die Ordnung des Basispunktes in E(F_p) nicht zu klein wird. Falls der Konnektor in der Rolle TLS-Client agiert, so MUSS er die eben genannten Ciphersuiten gegenüber RSA-basierten Ciphersuiten (vgl. GS-A_4384) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5256#7.4.1.2 ClientHello]).

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 ausschließlich TLS Version 1.2 (s. [87]). Insbesondere unterstützt der EVG alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS; dabei werden die Anforderungen aus [87] erfüllt. Die Kryptosuiten sollen für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt werden. Die TLS Versionen 1.1., 1.0 und SSL werden vom EVG nicht unterstützt. Falls der EVG in der Rolle als TLS-Client agiert, so wird er gem A_17124 die Ciphersuiten TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 undTLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 gegenüber anderen von ihm unterstützen RSA-basierte Ciphersuiten bevorzugen, d.h. in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5246#7.4.1.2 Client Hello]. Im Rahmen der Erstellung und Prüfung von digitalen Signaturen beim TLS-Handshakes unterstützt der EVG die folgende Hashfunktion: SHA-256. [FIPS-180-4].

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) *[none]*[177]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS.Zert The TSF shall use *interpretation rules*[178] 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

177 *[assignment: additional list of data types]*

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

ist. Ebenso muss sie anhand einer OCSP-Anfrage prüfen können, ob das Zertifikat noch gültig ist.

Anwendungshinweis 114: Die interpretation rules entsprechen der Konnektor-Spezifikation [92].

Anwendungshinweis 115: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [92] 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 [92]).

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

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

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

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* [179] 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*[180] that meet the following: *Standard RFC 5246 [59].*[181]

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

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

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

Anwendungshinweis 116: Der EVG unterstützt ausschließlich TLS Version 1.2 (s. [87]) Insbesondere werden vom EVG alle im SFR genannten cipher suites als Algorithmen für TLS unterstützt. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [19]) bzw. dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (ECDHE_RSA nach [60]). 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 [76]). Bezüglich Diffie-Hellman-Gruppen für die Schlüsselaushandlung wurden die Vorgaben aus [87] beachtet. Der DH-Exponent für den Schlüsselaustausch hat eine Mindestlänge gemäß [87]. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange werden die gemäß [87] 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

FCS_COP.1.1/NK.TLS.HMAC The TSF shall perform *HMAC value generation and verification*[182] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[183] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[184] that meet the following: *Standards FIPS 180-4 [14] and RFC 2104 [18]*[185].

Anwendungshinweis 117: FCS_COP.1/NK.TLS.HMAC wird für die Integritätssicherung innerhalb des TLS-Kanals benötigt.

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

[183] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/NK.TLS.AES Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.AES The TSF shall perform *symmetric encryption and decryption*[186] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[187] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[188] that meet the following: *FIPS 197 [15],* NIST 800-38D *[17],* RFC 5246, RFC 8422 *[60], RFC 5289 [61], specification [86]* [189].

Anwendungshinweis 118: Es gilt Anwendungshinweis 109.

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/AK.Enc.

Die *signature creation* wird in der Regel (Ausnahmen s.u.) 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 entweder im EVG erzeugt (FCS_CKM.1/NK.Zert) oder importiert

186 [assignment: *list of cryptographic operations*]

187 [assignment: *cryptographic algorithm*]

188 [assignment: *cryptographic key sizes*]

190 [assignment: *list of cryptographic operations*]

(FDP_ITC.2/AK.Enc). 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

(1) *verification of digital signatures and*

(2) *signature creation with support of gSMC-K storing the signing key and performing the RSA operation* [190]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[191] and cryptographic key sizes *2048 bit*[192] that meet the following: *RFC 8017 (RSASSA-PKCS1-v1_5) [31], FIPS PUB 180-4 [14]*[193].

Anwendungshinweis 119: Die Signaturberechnung gemäß FCS_COP.1/NK.TLS.Auth wird für die Berechnung digitaler Signaturen zur Authentikation bei TLS verwendet. Der EVG nutzt dafür bei Verbindungen ins lokale Netz (LAN) des Leistungserbringers die gSMC-K. Der dafür benötigt asymmetrische Schlüssel wurde während der Produktion der gSMC-K importiert oder generiert. 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.

Hinweis: Der EVG unterstützt über den in FCS_COP.1/NK.TLS.Auth genannten Algorithmus hinaus den folgenden Algorithmus:
* als TLS-Client: *ecdsa-with-SHA256* auf Basis der Kurve brainpoolP256r1.

ecdsa-with-SHA256 wird vom EVG im Zuge der ECC-Migration (vgl. [87], sec. 5.4) unterstützt. Zu den Hashalgorithmen zur Signaturprüfung vgl. auch Anwendungshinweis 113.

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

190 [assignment: *list of cryptographic operations*]

191 [assignment: *cryptographic algorithm*]

192 [assignment: *cryptographic key sizes*]

193 [assignment: *list of standards*]

FDP_ETC.2/AK.Enc können die Zertifikate und die zugehörigen privaten Schlüssel vom Administrator exportiert werden. Key distribution 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*][194] and specified cryptographic key sizes *2048 bit*[195] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [36], BSI TR-03116-1 [76]*.[196]

The TSF shall

(3) create a valid X.509 [37] certificate with the generated RSA key pair and

(4) create a PKCS#12 [38] file with the created certificate and the associated private key.[197]

Anwendungshinweis 120: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [*86*], Anforderung GS-A_4368 umsetzen. Die Verfeinerung zu FCS_CKM.1/NK.Zert soll die Möglichkeit zur Erzeugung von X.509 Zertifikaten für die TLS-geschützte Kommunikation mit Clientsystemen bieten. Ein Export dieser Zertifikate und der zugehörigen privaten Schlüssel ist Gegenstand von FDP_ETC.2/AK.Enc.

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/AK 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]

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

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

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

197 refinement

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

FDP_ITC.2.2/NK.TLS The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/NK.TLS The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/NK.TLS The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/NK.TLS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

1. *Die TSF importiert X.509 Zertifikate für Clientsysteme durch den Administrator über die Managementschnittstelle*

2. *[none]*.[199]

Anwendungshinweis 121: Gemäß FMT_MOF.1/AK wird die Steuerung, unter welchen Umständen der Import von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen.

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/AK 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.

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

199 *[assignment*: *additional importation control rules]*.

FDP_ETC.2.1/NK.TLS The TSF shall enforce the *Certificate-Export-SFP*[200] 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:

a) Die TSF exportiert X.509 Zertifikate für Clientsysteme und den zugehörigen privaten Schlüssel durch den Administrator über die Managementschnittstelle. Als Exportformat wird PKCS#12 verwendet.

b) [none]. [201]

Anwendungshinweis 122: Gemäß FMT_MOF.1/AK wird die Steuerung, unter welchen Umständen der Export von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen.

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[202] the functions ~~-~~ *Management of TLS-Connections required by the Anwendungskonnektor*[203]to *Anwendungskonnektor*[204].

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

201 *[assignment: additional exportation control rules]*

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

203 [assignment:*list of functions*]

204 [assignment: *the authorised identified roles*]

The following rules apply: For each TLS-Connection managed by the Anwendungskonnektor, only the Anwendungskonnektor can determine:

(1) Whether one or both endpoints of the TLS-connection need to be authenticated and which authentication mechanism is used for each endpoint.

(2)Whether the Konnektor or the remote IT-Product or both can initiate the TLS-Connection.

(3)Whether TLS 1.2 or TLS 1.3 (if provided) are used and which subset of the set of cipher suites as listed in FTP_ITC.1/NK.TLS is allowed for each connection.

(4)Whether a "Keep-Alive" mechanism is used for a connection.

(5)**Which data can or must be transmitted via each TLS-Connection.**

(6)**Whether the validity of the certificate of a remote IT-Product needs to be verified and whether a certificate chain or a whitelist is used for this verification.**

(7)Under which conditions a TLS-connection is terminated.

(8)**Whether and how terminating and restarting a TLS-connection using a Session-ID is allowed.**

(9)**Whether and under which conditions certificates and keys for TLS-Connections are generated and exported or imported.**

(10) [*none*] [205]

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. [206]

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.
Es wurden neben den Vorgaben des PPs keine weiteren Handlungsoptionen für den Anwendungskonnektor beschrieben.
Der Netzkonnektor nutzt TLS-Verbindungen auch zur Absicherung der lokalen Administrierung. Diese Verbindungen werden nicht im Sinne von FMT_MOF.1/NK.TLS gemanagt, sondern sind mit der Implementierung der Managementschnittstelle festgelegt.

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

Anwendungshinweis 124: Das im SFR beschriebene Mangement der TLS Verbindungen erfolgt durch den Anwendungskonnektor.

205 **[assignment: *additional rules*]**

206 refinement

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 Stapel- und Komfortsignatur) werden alle in der gSMC-K (nicht Teil des EVG) implementiert. 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,
- 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.
- Protokolle zur Nutzung des SGD im Rahmen des Zugriffs auf die elektronische Patientenakte (SGD-Protokoll)
- Protokoll (VAU-Protokoll) zur Kommunikation zwischen fachmodul ePA und dem Aktensystem der ePA.

Für alle Kryptoalgorithmen gelten die Festlegungen der TR-03116 [76] und der gematik-Spezifikation zu den anzuwendenden Kryptoalgorithmen [*86*].

Anwendungshinweis 125: Es gilt Anwendungshinweis 109.

6.3.1.1. Basisalgorithmen

Der Konnektor nutzt kryptographische Dienste der gSMC-K in der Einsatzumgebung.

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 in accordance with a specified cryptographic algorithm SHA-256, SHA-384 und SHA-

512 and cryptographic key sizes none that meet the following: Standard FIPS PUB 180-4 [14].

Anwendungshinweis 126: Die Hashfunktionen SHA-256 werden durch den Signaturdienst benutzt.

Anwendungshinweis 127: Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren. Dabei werden die Vorgaben aus A_17768 umgesetzt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17207 und A_17359 erfüllt.

Cryptographic key generation / AES keys

FCS_CKM.1/AK.AES	
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 Entnahme aus Zufallszahlengenerator[207] and specified cryptographic key sizes 128 bit and 256 bit that meet the following: none[208].

Anwendungshinweis 128: Der Schlüssel wird erzeugt, indem die entsprechende Anzahl von Bits dem Zufallszahlengenerator, den die Einsatzumgebung bereit stellt (OE.NK.RNG), entnommen werden.

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_CKM.4.1/AK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method Überschreiben durch fixe Werte[209] that meet the following: none[210].

[207] [assignment: Algorithm for cryptographic key generation of AES keys]

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

[209] [assignment: *cryptographic key destruction method*]

[210] [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 [25] [43], CAdES [26] [44], PAdES [27] [45] und mit PKCS#1-Containern, PKCS#1v2.2, [31]. Der EVG prüft signierte Dokumente nach den angegebenen Standards und die bei der Stapelsignatur von den Chipkarten erzeugten digitalen Signaturen.

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 in accordance with a specified cryptographic algorithm RSASSA-PKCS1-v1_5 signature verification and cryptographic key sizes 1976 bit to 4096 bit that meet the following: Standard PKCS#1 [31].

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 bei nicht-qualifizierten elektronischen Signaturen auf die exakte Schlüssellänge 2048 bit geprüft wird, vgl. Tabelle 31. Dabei werden die Vorgaben aus A_17768 erfüllt.

Anwendungshinweis 130: Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren. Dabei werden die Vorgaben aus A_17768 umgesetzt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17207 und A_17359 erfüllt.

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 in accordance with a specified cryptographic algorithm RSASSA-PSS signature verification and cryptographic key sizes 1976 bit to 4096 bit that meet the following: Standard PKCS#1v2.2, [31].

Anwendungshinweis 131: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.PSS wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierter elektronischen Signaturen verwendet, wobei bei nicht-qualifizierten elektronischen Signaturen auf die exakte Schlüssellänge 2048 bit geprüft wird, vgl. Tabelle 31 Dabei werden die Vorgaben aus A_17768 erfüllt.

Anwendungshinweis 132: Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren. Dabei werden die Vorgaben aus A_17768 umgesetzt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17207 und A_17359 erfüllt.

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 in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 256 bit that meet the following: Standard TR-03111 [74].

Hinweis: Der Konnektor unterstützt zur Signaturprüfung den in [93] angegebenen Signaturalgorithmus *ecdsaWithSha256* (OID 1.2.840.10045.4.3.2) auf der Kurve brainpoolP256r1 nach RFC 3279 [64] und RFC 5639 [64].

Anwendungshinweis 133: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.ECDSA wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet, vgl. [*86*]. Dabei werden die Vorgaben aus A_17768 erfüllt.

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 **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm (1) XML Advanced Electronic Signature (XAdES), (2) SAML2

(3) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS

and cryptographic key sizes no key that meet the following: Standards XMLSig [22], XAdES[25] [43], SAML2 [70] and FIPS PUB 180-4 [14].

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 PKCS#1v2.2 PSS, geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel. Die Vorgaben aus A_17768 werden erfüllt.
Im Fall von XML-Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17206 und A_17360 erfüllt.
Im Fall von Signaturen von SAML-Token (SAML2) muss der EVG die Signaturvariante „enveloped“ umsetzen und sicherstellen, dass 1) das gesamte Input XML signiert wird und 2) die Signatur direktes Child-Element des Root-Elements wird. Die Schnittstelle zur Signatur von SAML-Token muss vom EVG so umgesetzt werden, dass diese nur intern und durch Fachmodule genutzt werden kann. Die Vorgaben aus A_19052 in [93] bzgl. der Profilierung der verarbeiteten Dokumente und Nachrichten werden umgesetzt (Ausnahmen: 1. Die Anforderung „Bei Referenzen (ReferenceType) darf das Optionale URI-Attribut nicht vorhanden sein oder es muss leer sein.“ wird wie folgt implementiert: „Bei Referenzen (ReferenceType) dürfen sich im optionalen URI-Attribut keine "xpointer()"-Ausdrücke befinden." 2. Es werden 10 Transformationen pro Reference-Element (max. 10 Reference-Elemente) unterstützt).

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 **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 and cryptographic key sizes no key that meet the following: Standards RFC5652[34], CAdES [26] [44] and FIPS PUB 180-4 [14].

Anwendungshinweis 135: FCS_COP.1/AK.CMS.Sign fordert die Erzeugung von CMS-Signaturen nach vorgegebenen Signaturrichtlinien. 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 zukünftig ECDSA), geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel. Die CMS-Signaturen werden ebenfalls in S/MIME-Nachrichten verwendet. Dabei sind die Vorgaben aus A_17768 umgesetzt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17207 und A_17359 erfüllt.

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 **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 and cryptographic key sizes no key that meet the following: Standards PAdES [27] [45] and FIPS PUB 180-4 [14].

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 PKCS#1 PSS und RSA 2048Bit-Schlüsseln, geleistet werden. Im Fall von Signaturen auf Basis von ECC müssen die Vorgaben aus A_17208 eingehalten werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel. Dabei werden die Vorgaben aus A_17768 erfüllt.

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 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 for QES according to FCS_COP.1/AK.SigVer.PSS,

and cryptographic key sizes 1976 bit to 4096 bit for RSA[211],

(3) SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA[212] and cryptographic key sizes 256 bit for QES

that meet the following: Standards XMLSig[21], XAdES [25] [43], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [74].

Anwendungshinweis 137: FCS_COP.1/AK.XML.SigPr fordert die Prüfung von qualifizierten XML-Signaturen nach vorgegebenen Signaturrichtlinien und den bereits oben spezifizierten Kryptoalgorithmen. Die Prüfung von nicht-qualifizierten oder anderen Signaturalgorithmen, die über BSI-CC-PP-0098-V3 hinausgehen, wird nicht unterstützt. Dabei werden die Vorgaben aus A_17768 erfüllt. Im Fall von XML-Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17206 und A_17360 erfüllt. Die Vorgaben aus A_19052 in [93] bzgl. der Profilierung der verarbeiteten Dokumente und Nachrichten werden umgesetzt (Ausnahmen: 1. Die Anforderung „Bei Referenzen (ReferenceType) darf das Optionale URI-Attribut nicht vorhanden sein oder es muss leer sein.“ wird wie folgt implementiert: „Bei Referenzen (ReferenceType) dürfen sich im optionalen URI-Attribut keine "xpointer()"-Ausdrücke befinden." 2. Es werden 10 Transformationen pro Reference-Element (max. 10 Reference-Elemente) unterstützt).

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 in accordance with a specified cryptographic algorithm (1) CMS Advanced Electronic Signature (CAdES),

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

[212] [assignment: *cryptographic algorithm*]

(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,

and cryptographic key sizes 1976 bit to 4096 bit for for QES and 2048 Bit for nonQES,

(3) SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA and cryptographic key sizes 256 bit for QES and nonQES

that meet the following: Standards RFC5652[34], CAdES [26] [44], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [74].

Anwendungshinweis 138: FCS_COP.1/AK.CMS.SigPr fordert die Prüfung von CMS-Signaturen nach vorgegebenen Signaturrichtlinien und den bereits oben spezifizierten Kryptoalgorithmen. Bei nicht-qualifizierten elektronischen Signaturen wird ausschließlich FCS_COP.1/AK.SigVer.PSS (Schlüssellänge exakt 2048 bit) in Kombination mit SHA-256 umgesetzt, vgl. Tabelle 31. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren. Dabei werden die Vorgaben aus A_17768 umgesetzt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17207 und A_17359 erfüllt.

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 in accordance with a specified cryptographic algorithm (1) PAdES [27] [45], (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, and cryptographic key sizes 1976 bits to 4096 bits for QES and 2048 Bit for nonQES,

(3) SHA-256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA and cryptographic key sizes 256 bit for QES and nonQES[213]

that meet the following: Standards PAdES [27] [45], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [74].

Anwendungshinweis 139: FCS_COP.1/AK.PDF.SigPr fordert die Prüfung von PDF-Signaturen nach vorgegebenen Signaturrichtlinien und den bereits oben spezifizierten Kryptoalgorithmen. Bei nicht-qualifizierten elektronischen Signaturen wird ausschließlich FCS_COP.1/AK.SigVer.PSS (Schlüssellänge exakt 2048 bit) in Kombination mit SHA-256 umgesetzt, vgl. Tabelle 31. Dabei werden die Vorgaben aus A_17768 umgesetzt. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signatur¬erstellungs¬zeitpunkt noch gültig waren. Dabei werden die Vorgaben aus A_17768 erfüllt. Im Fall von Signaturen auf Basis eines ECC-Schlüssels werden die Vorgaben aus A_17208 erfüllt.

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 in accordance with a specified cryptographic algorithm AES-GCM and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards FIPS 197 [15], ~~NIST-SP-800-38A~~ NIST-SP-800-38D [17][214].

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

[214] [assignment: *list of standards*]; Korrektur von BSI-CC-PP-0098-V3, da für den Modus GCM nur [17] relevant ist

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.MIME.Ver bzw. FCS_COP.1/AK.MIME.Ent, FCS_COP.1/AK.CMS.Ver, bzw. FCS_COP.1/AK.CMS.Ent benötigt. Die Schlüssellänge 192 Bits wird 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. Bei Verwendung von AES für die Ver- und Entschlüsselung muss der EVG die Vorgaben aus A_18001 und A_18002 unterstützen.

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 in accordance with a specified cryptographic algorithm RSAOAEP, ECIES (in accordance with chapter 5.7 in [86]) with a key length of 256 Bit and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 256 bit for AES and 2048 bit for RSA that meet the following: Standards NIST-SP-800-38D [17], PKCS#1 [31], FIPS 197 [15] und XMLEnc [21].

Anwendungshinweis 142: > Auf Grund der besonderen Gegebenheiten in der TI muss der EVG auch im Kontext ECIES zunächst ein AES-Verschlüsselung des Payloads mittels eines 256Bit langen Schlüssels vornehmen. Die genaue Vorgehensweise ist in Kapitel 5.7 in [86] und muss unbedingt beachtet werden (siehe auch A_17221).

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 in accordance with a specified cryptographic algorithm ***RSAOAEP, ECIES*** (in accordance with chapter 5.7 in [87]) with a key length of 256 bit and AES-GCM with authentication tag length of 128 bit and

cryptographic key sizes 128 bit, 192bit and 256 bit[215] that meet the following: Standards NIST-SP-800-38D [17], FIPS 197 [15] und XMLEnc [21].

Anwendungshinweis 143: Die asymmetrische Entschlüsselung des AES-Schlüssels mit privaten Schlüsseln gemäß RSA OAEP (s. [79]) und ECIES erfolgt durch die Chipkarte der Einsatzumgebung (HBA, SMC-B oder ggf. eGK). Im Fall von kartenbasierter Entschlüsselung werden die Vorgaben in A_17746 erfüllt.

FCS_COP.1/AK.MIME.Ver	**Cryptographic operation / MIME 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.MIME.Ver	The TSF shall perform encryption of MIME documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 256 bit for AES and 2048 bit for RSA that meet the following: Standards NIST-SP-800-38D [17], PKCS#1 [31], FIPS 197 [15] und RFC 5751 [35].
Hinweis:	Im Fall von kartenbasierter Verschlüsselung (HBA, SMC-B oder ggf. eGK) werden die Vorgaben aus A_17746 umgesetzt.

FCS_COP.1/AK.MIME.Ent	**Cryptographic operation / MIME 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.MIME.Ent	The TSF shall perform decryption of MIME documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm ***RSAOAEP***[216] and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 128 bit, 192bit and 256 bit that meet the following:

[215] [**Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP, ECIES***]

[216] [**Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP, ECIES***]

Standards NIST-SP-800-38D [17], PKCS#1 [31], FIPS 197 [15] und RFC 5751 [35].

Anwendungshinweis 144: Die asymmetrische Entschlüsselung des AES-Schlüssels mit RSAOAEP (s. [79]) erfolgt durch die Chipkarte der Einsatzumgebung (HBA, SMC-B oder ggf. eGK).

Anwendungshinweis 145: Für die S/MIME Ver- und Entschlüsselung muss statt des in RFC 5751 beschriebenen CMS Data Content Type mit AES-CBC Verschlüsselung (Section 2.4 und 2.7) der CMS Authenticated-Enveloped-Data Content Type gemäß RFC 5083 mit AES-GCM Inhaltsverschlüsselung gemäß RFC 5084 verwendet werden. Im Fall von kartenbasierter Entschlüsselung (HBA, SMC-B oder ggf. eGK) wird A_17746 umgesetzt.

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 in accordance with a specified cryptographic algorithm RSAOAEP, ECIES (in accordance with chapter 5.7 in [86] and a kex length of 256 bit) and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 256 bit for AES and 2048 bit for RSA that meet the following: Standards NIST SP800-38D [17], PKCS#1 [31], FIPS 197 [15] and CMS [34].

Anwendungshinweis 146: Auf Grund der besonderen Gegebenheiten in der TI muss der EVG auch im Kontext ECIES zunächst eine AES-Verschlüsselung des Payloads mittels eines 256 Bit langen Schlüssels vornehmen. Die genaue Vorgehensweise ist in Kapitel 5.7 in [87] beschrieben.

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 in accordance with a specified cryptographic

algorithm ***RSAOAEP***[217]**, *ECIES*** (in accordance with chapter 5.7 in [86] with a key length of 256 bit) and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST SP800-38D [17], PKCS#1 [31], FIPS 197 [15] and CMS [34].

Hinweis: Im Fall einer ECC-basierten Entschlüsselung werden die Vorgaben aus A_17220 erfüllt. Im Fall von kartenbasierter (HBA, SMC-B oder ggf. eGK) Entschlüsselung werden die Vorgaben in A_17746 erfüllt.

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 • Ein Passwort muss Zeichen aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern enthalten. Ein valides 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 Verwendung eines der drei letzten Passwörter beim Passwortwechsel durch den Benutzer selbst ist nicht zulässig (Passworthistorie). [218].

[217] [**Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP, ECIES***]

[218] [assignment: a defined quality metric]

Anwendungshinweis 147: Die Verfeinerung von „Geheimnisse“ zu „Passwörtern“ ist notwendig, um die Qualitätsanforderungen gegenüber anderen Mechanismen abzugrenzen. Gemäß [92], Kap. 4.3.1, sind Administratorpasswörter gefordert, die den Anforderungen aus dem IT_Grundschutz-Katalog des BSI genügen. Mindestens diese Anforderungen sind durch das assignment "a defined quality metric" in FIA_SOS.1/AK.Passwörter umgesetzt.

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.
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.

FIA_UID.1/AK	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/**AK**	The TSF shall allow (1) Self test according to FPT_TST.1/AK.Out-Of-Band, (2) none[219] 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: Die vorliegenden Sicherheitsvorgaben weisen keine TSF-vermittelten Aktionen zu, die nicht bereits im zugrundeliegenden Schutzprofil BSI-CC-PP-0098-V3 aufgeführt sind. An der Schnittstelle zur lokalen Administration, wodurch eine implizite Identifikation stattgefunden hat, kann statt der Benutzerdaten (Nutzername und Passwort) eine Zeichenkette, die für jeden Konnektor verschieden ist und dem Gerät bei Auslieferung beiliegt, eingegeben werden. Bei korrekter Eingabe findet dann ein Werksreset statt.

FIA_UAU.1/AK	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

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

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) none[220]

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: Die vorliegenden Sicherheitsvorgaben weisen keine TSF-vermittelten Aktionen zu, die nicht bereits im zugrundeliegenden Schutzprofil BSI-CC-PP-0098-V3 aufgeführt sind.
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.

FIA_UAU.5/AK Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/AK The TSF shall provide

(1) password based authentication mechanism in case of local administration[221] for administrator users,

(2) TLS authentication with a pairing secret for eHKT [92], 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,

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

221 [selection: password based authentication mechanism [assignment: another authentication mechanism]]

(5) UUID-based authentication mechanism in case of a comfort signature creation

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.

(7) The TSF shall authenticate the user when creating a comfort signature by the validation of the UUID presented by S_Client.

Die Validierung der vom Clientsystem dem EVG präsentierten UUID erfolgt hinsichlich ihrer Beschaffenheit und Länge (UUID gem. RFC4122, min. 128 Bit Länge gemäß A_20073-01 in [93] und ihrer Anwendungskontext-übergreifende Eindeutigkeit über die letzten 1000 Vorgänge (vgl. A_20074 in [93]).

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 (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 to prove the identity of the "SAK".

Anwendungshinweis 151: Diese SFR ergibt sich aus der TR-03114 [75], A_19258 in [93] und den Zugriffsbedingungen des HBA, die für eine Stapel- oder Komfortsignatur die Authentisierung der Identität „SAK" gegenüber dem HBA und die Übermittlung der DTBS mit Secure Messaging erfordern. Die gSMC-K muss dafür über ein CVC mit der CHAT für die Identität „SAK" (vergl. C.SAK.AUTD_CVC in [101]) und den dazugehörigen privaten Schlüssel PrK.SAK.AUTD_CVC verfügen. Für eine Beschreibung des externen Verhaltens des EVG im Authentisierungsprotokoll mit dem HBA wird auf [75], [97], [99] und [101] verwiesen.

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 die Tabellen im Abschnitt 9.1.

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 on the subject S_Clientsystem, the objects as in TAB_KON_507, and the operation: • usage of the resource (the object) in a technical use case.
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 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.
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.
FDP_ACF.1.3/AK.Infomod	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[222].
FDP_ACF.1.4/AK.Infomod	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[223].

FMT_MSA.1/AK.Infomod	**Management of security attributes / Informationsmodell**

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

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

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.Infomod	The TSF shall enforce the Infomodell-SFP to restrict the ability to modify, delete, create 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 to S_Administrator.
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 to provide restrictive[224] 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[225] to specify alternative initial values to override the default values when an object or information is created.

6.3.3.2. Kartenterminaldienst

Der Anwendungskonnektor kommuniziert mit den konfigurierten eHealth-Kartenterminals über gesicherte Kanäle. Der EVG stellt diese Kommunikationskanäle kontrolliert dem EVG zur Verfügung.

FDP_ACC.1/AK.eHKT	**Subset access control / Kartenterminaldienst**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

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

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

FDP_ACC.1.1/AK.eHKT The TSF shall enforce the Kartenterminaldienst-SFP 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.

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 FCS_COP.1/NK.HMAC.	Die TLS-Kanäle sind in [92] und [94] beschrieben. Die gesamte Kommunikation des Konnektors mit den eHealth-Kartenterminals erfolgt über die TLS-Kanäle des Kartenterminaldienstes.
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	

Operation	Beschreibung	Anmerkung
SICCT-Kommando senden	Übermittlung eines SICCT-Kommandos gemäß [96] und [94]über den TLS-Kanal an ein eHealth-Kartenterminal,das durch den Chipkartendienst selbst erzeugt oder an den Kartenterminaldienst übergeben wurde	Die SICCT-Kommandos dienen [94] [96] - 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 Chipkarten-kontaktiereinheiten 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 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.

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.

(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.

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.

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.

(2) none[226]

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 to transmit and receive ~~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 to transmit and receive user data ~~**in a manner**~~ protected from modification, deletion, insertion, replay errors.
FDP_UIT.1.2/AK.TLS	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay has occurred.

FMT_MTD.1/AK.eHKT_Abf	**Management of TSF data / eHealth-Kartenterminal Abfrage**
Hierarchical to:	No other components.
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 the Arbeitsplatzkonfigurationsdaten:

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

(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.

to S_AK and S_Administrator.

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 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) Import von eHealth-Kartenterminal-Informationen nach Anzeige und Bestätigung to S_Administrator.

Anwendungshinweis 152: Die Iteration differenziert die Zugriffsbedingungen für das Management der Konfigurationsdaten nach Zugriffsarten und Rollen. Das Management der Kartenterminals ist in [92] 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 [92], Kap 4.3.3, beschrieben.

6.3.3.3. Chipkartendienst

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. [92]). Die Identifikation dieser Chipkarten erfolgt durch Kartenhandles. Der EVG stellt Sicherheitsfunktionen des Chipkartendienstes bereit.

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 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, (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.

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 Sicherheitsattribute 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 ö 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).	
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.
Chipkartenkommando übertragen und Antwort empfangen	Übertragung von Chipkartenkommandos und das Empfangen von Antworten innerhalb von SICCT-Kommandos des Kartenterminaldienstes	
Benutzerauthentisie-rung 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 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”.
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) Das Subjekt 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 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 das Subjekt S_AK, der 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) Das Subjekt S_AK und S_Fachmodul, das den logischen Kanal angefordert hat, darf die Schließung eines 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.

FDP_ACF.1.3/AK.KD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[227]

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.[228]

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 [92], Kap. 4.1.5.4, definiert.

FDP_ACC.1/AK.PIN Subset access control / PIN

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

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

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 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.

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 [92], 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 [92], Kap. 4.1.5, und [75] 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 [96] und [94] 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 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,

(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.

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.

(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 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,

FDP_ACF.1.3/AK.PIN The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[229]

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

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

(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 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[230]

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. [77]) durch das Clientsystem ist nicht gestattet.
Gemäß TAB_KON_047 ist die Operation VerifiyPin an der Außenschnittstelle ausschließlich für PIN.CH des HBA oder PIN.SMC der SMC-B erlaubt.

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.
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.

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

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. [92], Kap. 4.1.8.1.3). Dies entspricht $1,76 \cdot 10^7$ möglichen Jobnummern. Laut [92] wird die Jobnummer vom Konnektor erzeugt und kann durch Clientsysteme abgerufen werden. Der Konnektor soll jedoch laut [92] 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 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.

Operation	**Beschreibung**	**Anmerkung**
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 Signaturschlüssel 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/AK.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. Abweichend davon wird der Signatur-PIN-Authentisierungsstatus der Signaturkarte im Fall der Komfortsignatur nicht nach jeder Signatur zurückgesetzt sondern wenn a) SAK_COMFORT_SIGNATURE deaktiviert wird (vgl. A_19105, Schritt 2 in [93]), b) der Zähler SAK_COMFORT_SIGNATURE_TIMER den eingestellten Maximalwert erreicht hat (vgl. A_18686 und A_19103 Schritt 2 in [93]), wobei gem A_18686 laufende Signatturstapel vollständig abgearbeitet werden, c) der Zähler SAK_COMFORT_SIGNATURE_MAX den eingestellten Höchstwert erreicht hat (vgl. A_19100 und A_19102 Schritt 3 in [93]) oder d) die Operation DeactivtaeComfortSignature aufgerugen wird (vgl. A_19105, Schritt 5a in [93]).

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 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.

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 Signaturdienst steuert den Signaturprozess des identifizierten Arbeitsplatzes.
(3) Das Subjekt Signaturdienst darf nur dann die zu signierenden Dokumente signieren, wenn
   (a) der Sicherheitsstatus der Signaturchipkarte die Erzeugung der digitalen Signatur erlaubt,
   (b) im Fall der Komfortsignatur die Konfiguration SAK_COMFORT_SIGNATURE global auf „enabled“ gesetzt ist,
   (c) im Fall der Komfortsignatur der Aufrufkontext und die UserID des S_Benutzer_geprüft und positiv gegen jene beim Aufruf von ActivateComfortSignatur für die zu nutzende Signaturkarte abgeglichen wurden (vgl. TIP1-A_4524-02 Regel 9 und TAB_KON_514(-01)[231] in [93]),

[231] Abweichend von TAB_KON_514-01 werden die Fehlercodes 4004, 4005 und 4006 an der Außensschnittstelle des EVG ausgegeben.

(d) Im Fall der Komfortsignatur die UserID von S_Benutzer eine Länge von min. 128 Bit aufweist, eine UUID gem. RFC4122 ist (vgl. A_20073-01 in [93]) und die UserID eindeutig ist (vgl. A_20074 in [93])

(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 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 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 „identifizierte Benutzer des Clientsystems“ darf den Signaturvorgang für die autorisierten zu signierenden Dokumente abbrechen,

(f) der Signaturdienst darf nur ordnungsgemäß signierte Dokumente an den S_AK zurückgeben,

(g) das Subjekt Signaturdienst muss nach Abarbeitung des Stapels, bei Abbbruch des Signaturvorgangs durch das Subjekt „identifizierte Benutzer des Clientsystems“ und bei festgestellten ungültig signierten Dokumente den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA zurücksetzen.

(h) Abweichend von Buchstabe g): Das Subjekt Signaturdienst setzt im Fall der Komfortsignatur den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA nicht nach jeder Signatur zurück sondern wenn a) SAK_COMFORT_SIGNATURE deaktiviert wird (vgl. A_19105, Schritt 2 in [93]), b) der Zähler SAK_COMFORT_SIGNATURE_TIMER den eingestellten Maximalwert erreicht hat (vgl. A_18686 und A_19103 Schritt 2 in [93]), wobei gem A_18686 laufende Signatturstapel

vollständig abgearbeitet werden, c) der Zähler SAK_COMFORT_SIGNATURE_MAX den eingestellten Höchstwert erreicht hat (vgl. A_19100 und A_19102 Schritt 3 in [93]) oder d) die Operation DeactivtaeComfortSignature aufgerufen wird (vgl. A_19105, Schritt 5a in [93]).

(5) Wenn die gültige Signaturrichtlinie die Erstellung einer qualifizierten elektronischen Signatur verlangt, darf das Subjekt Signaturdienst nur ordnungsgemäße qualifizierte elektronische Signaturen an den S_AK zurück geben.

(6) Das Subjekt S_AK darf dem Signaturdienst Binärstrings mit der maximalen Länge von 512 Bit nur 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.

(7) Das Subjekt S_AK darf eine Komfortsignatur nur anbieten und durchführen, wenn die Konfiguration SAK_COMMFORT_SIGNATURE auf den Wert „enabled“ gesetzt ist (vgl. A_19104 A_19103 in [93]).

FDP_ACF.1.3/AK.Sgen The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[232].

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 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 identifizierten Benutzers des Clientsystems fehlschlägt.

(2) Das Subjekt 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.

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

(3) Das Subjekt 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 Signaturdienst darf kein Subjekt auf

(a) das Verzeichnis DF.QES des HBA,

(b) den Schlüssel PrK.HCI.OSIG der SMC-B,

(c) none[233]

zugreifen.

(5) none[234].

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. Die im Fall der Komfortsignatur verwendete UserID muss vom EVG im Sinne eines Authentisierungsgeheimnisses behandelt und gegen eine Offenlegung geschützt werden.
Im Handbuch zum EVG ist ein Hinweis zum Beitrag des Primärsystems (Clientsystem) zur Sicherheit der Komfortsignatur durch die sichere Nutzer-Authentisierung und die Generierung einer starken UserID enthalten (vgl. A_19101 in [93]).

Anwendungshinweis 157: Die Bedingungen für die Sicherheitsattribute signierter Dateien „ordungsgemäß“ und „ungültig“ sind durch FMT_MSA.4/AK festgelegt.

Anwendungshinweis 158: Die SFR **FDP**_ACF.1/AK.Sgen erfasst die von BSI-CC-PP-0098-V3 vorgesehenen Signaturarten sowie die Komfortsignatur.

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 on subjects: (1) S_AK, (2) S_Signaturdienst, (3) S_Benutzer_Clientsystem;

[233] [assignment: *weitere Signaturschlüssel externer Signaturchipkarten*]

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

objects:

(1) Signierte Dokumente,
(2) Signaturprüfungsergebnis;

operations:

(1) Signatur prüfen,
(2) Festlegen des angegebenen Zeitpunkts.

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 to objects based on the following **list of subjects, objects and security attributes**: subjects: (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.
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.

FDP_ACF.1.3/AK.SigPr	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[235].
FDP_ACF.1.4/AK.SigPr	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[236].

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 [92] 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
  - falls vorhanden Ermittelter_Signaturzeitpunkt_Eingebettet, sonst
  - Ermittelter_Signaturzeitpunkt_System.

Bei der QES-Signaturprüfung wird ein ggf. vorhandener qualifizierter Zeitstempel 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 **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 [42] oder ISO-8859-15 [11]),** **(2) TIFF-Dateien [41],** **(3) Adobe Portable Document Format (PDF/A) [12] [13],** **(4) XML-Dateien [20] [24]** **und die Formate signierter Daten**

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

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

(1) PAdES [27] [45] **für PDF/A-Dokumente,**

(2) CAdES [26] [44] für XML, PDF/A, Text und TIFF Dokumente,

(3) XAdES [25] [43] 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 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 [74] und PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v1_5 [31].**

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[237],

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,

[237] [selection: none, qualifizierter Zeitstempel über die Signatur]

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[238]**.**

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 [92] schränkt die zu unterstützenden Kombinationen der Dokumentenfromate, Formate signierter Daten und Signaturvarianten ein (vgl. Tabelle 31 dieser Sicherheitsvorgaben). 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.
Der EVG muss sowohl bei der Erstellung als auch der Prüfung qualifizierter Komfortsignaturen die Vorgaben aus TUC_KON_778 in [93] bzgl. des Einsatzbereiches der Signaturvarianten einhalten (vgl. A_19945 in [93]).

238 **[assignment: *andere Form von Nachweisen*]**

Anwendungshinweis 161: Bei QES werden für die Prüfung der Zertifikate, die OSCP-Antworten und die OCSP-Zertifikate die folgenden Verfahren unterstützt:
* **RSASSA-PKCS1-v1_5** (Schlüssellänge 1976-4096 Bit) mit
** SHA-256 (sha256WithRSAEncryption, OID 1.2.840.113549.1.1.11),
** SHA-384 (sha384WithRSAEncryption, OID 1.2.840.113549.1.1.12),
** SHA-512 (sha512WithRSAEncryption, OID 1.2.840.113549.1.1.13)
* **RSASSA-PSS** (OID1.2.840.113549.1.1.10) (Schlüssellänge 1976-4096 Bit) mit SHA-256, SHA-384, SHA-512. Für **RSASSA-PSS** sind für die Kombination mit Hashalgorithmen keine OIDs definiert. Die Information über die zu verwendende Hashfunktion erfolgt anhand der Parameter der Signatur.
* ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf brainpoolP256r1 (256 Bit Schlüssellänge).

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“ wie in FDP_DAU.2.1/AK.QES genannt.

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 **durch nicht-qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der Chipkarten**. **Es sind die Dokumentenformate zu signierender Daten** **(1) Text-Dateien (UTF-8 [42] oder ISO-8859-15 [11]),** **(2) TIFF-Dateien[41],** **(3) Adobe Portable Document Format (PDF/A) [12],** **(4) XML-Dateien [20] [24],** **(5) MIME [35],** **(6) Binärdokument,** **und die Formate signierter Daten** **(1) PAdES [27] [45] für PDF/A-Dokumente,** **(2) CAdES [26] [44] für Text, TIFF, Adobe Portable Document Format (PDF/A) und XML Dokumente sowie Binärdokumente,** **(3) S/MIME [35],** **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* 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 [74], PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [31] 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[239].

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. Die definierte Zuweisung ist in diesen Sicherheitsvorgaben leer. Zum Nachweis der erfolgreichen Prüfung müssen die für die Gültigkeitsprüfung benutzten OCSP-Antworten mit einem Zeitstempel versehen und dem Nutzer zugänglich gemacht werden. Über die Signaturrichtlinie NFDM und den in FDP_DAU.2/AK.Sig sowie BSI-CC-PP-0098-V3, Abschnitt 1.3.5.2, hinaus werden keine weiteren Signaturrichtlinien unterstützt. Vgl. Tabelle 31 dieser Sicherheitsvorgaben für eine Übersicht der unterstützten Formate für nicht-qualifizierte elektronische Signaturen.

239 **[assignment: *andere Form von Nachweisen*]**

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: Bei nicht-qualifizierten Signaturen wird für die Prüfung der Zertifikate, die OCSP-Antworten und die OCSP-Responder-Zertifikate wird ausschließlic sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf der Kurve brainpoolP256r1 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.
FDP_DAU.2.2/AK.Cert	The TSF shall provide *S_Benutzern* 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,** **(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[240].**

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.

[240] **[assignment: *andere Form von Nachweisen*]**

Anwendungshinweis 168: Bei nicht-qualifizierten Signaturen wird für die Prüfung der Zertifikate, die OCSP-Antworten und die OCSP-Responder-Zertifikate wird ausschließlic sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) und ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) auf der Kurve brainpoolP256r1 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 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.
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.
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 to provide restrictive 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 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
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 on all objects, based on the following attributes: Korrektheit des Hashwertvergleichs[241].
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) Sobald die Daten, die zu signieren sind, den Signaturdienst vollständig erreicht haben, wird darüber gem. FCS_COP.1/NK.Hash ein Hash berechnet. Nach Erzeugung der Signatur muss diese erneut auf mathematische Korrektheit geprüft werden, bevor das Ergebnis den Signaturdienst verlassen darf. Im Fehlerfall ist lediglich ein entsprechender Fehler zu retournieren.[242].

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 ist 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.

[241] [assignment: *user data attributes*]

[242] [assignment: *action to be taken*]

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 to restrict the ability to (1) Modify the security attribute Autorisierungsstatus zu signierender Daten, **(2) Select the security attribute gültige Signaturrichtlinie für zu signierende Daten,** **(3) Modify the security attributes angegebener Zeitpunkt signierter Daten für die Signaturprüfung** to S_Benutzer_Clientsystem.

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 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.

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**
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

Siehe Abschnitt 6.2.6, FDP_ACC.1/NK.Update, FDP_ACF.1/NK.Update und FDP_UIT.1/NK.Update.

Anwendungshinweis 175: Die Liste der zulässigen Software-Versionen wird in der Spezifikation Einführung der Gesundheitskarte. Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM] mit “Firmware-Gruppe” bezeichnet [103]. Diese muss als versionierte Liste zulässiger Firmware-Versionen für Software-Updates in jede Konnektor-Software integriert werden.

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 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.

Operation	**Beschreibung**
Verschlüsseln	Hybridverschlüsselung von XML-Dokumenten gemäß FCS_COP.1/AK.XML.Ver, MIME nach FCS_COP.1/AK.MIME.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 Entschlüsselung gemäß FCS_COP.1/AK.XML.Ent, SMIME nach FCS_COP.1/AK.MIME.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 22: 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 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[243].

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:

(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

[243] [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*]

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.[244]

FDP_ACF.1.3/AK.Enc The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[245].

FDP_ACF.1.4/AK.Enc The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[246].

Anwendungshinweis 176: Die vorliegenden Sicherheitsvorgaben haben die offenen Operationen, die das zugrundeliegende Schutzprofil lässt, ausgeführt. Alle Verschlüsselungsrichtlinien 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 Anwendungen 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 when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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 vorgehenen Empfänger. (3) Die TSF importiert TI-fremde X.509 CA-Zertifikate durch den Administrator über die Managementschnittstelle.

Anwendungshinweis 177: Die Verschlüsselungsrichtlinie ist eindeutig durch die Fachanwendung bzw. innerhalb der Fachanwendung durch den Anwendungsfall festgelegt und muss dem Verschlüsselungsdienst 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 mit 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 Verschlüsselungs-SFP 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[247].

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:

- 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 [93] 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 250, eine explizit verbietende Regel für die Zuweisung, die BSI-CC-PP-0098-V3 vorsieht, eingesetzt wurde.

FDP_ACC.1/AK.TLS	**Subset access control / TLS-Kanäle**
Hierarchical to:	No other components.

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

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK.TLS	The TSF shall enforce the AK-TLS-SFP 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, (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.

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_Fachmodul 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 und S_	Algorithmen und Schlüssel für die Kanalverschlüsselung werden mit dem Kommunikationspartner ausgehandelt. Dem TLS-Kanal wird ein TLSConnectionIdentifier zugeordnet.

Operation	Beschreibung	Anmerkung
	Fachdienst nutzt stets das X.509 Zertifikat C.FD.TLS-S für die Server-Authentisierung. (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. [92], Kap. 3.4). Der EVG nutzt in diesem Fall das Schlüsselmaterial der Identität des X.509 Zertifikats C.AK.AUT der gSMC-K. (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. (5) Bei allen TLS-Verbindungen muss zur Authentifizierung eine X.509-Identität gemäß GS-A_4359 in [87] verwendet werden.	
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 einer TLS-Verbindung (nur VSDM)	Das S_Fachmodul (VSDM) fordert die Wiederaufnahme der Sitzung des Kanals unter Verwendung des Session-ID gemäß RFC 5246, Kap. 7.3, beim Intermediär VSDM an.	Der Intermediär VSDM kann die Wiederaufnahme der Sitzung 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 23: 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 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, (3) TLS-Kanal with the security attribute „Anfordernder TLS-Client".
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 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 einen TLS-Kanal zum TSL-Dienst auf.

(12) Der S_AK baut für den Download der Hash-Datei der TSL(ECC-RSA) eine TLS-Verbindung zum S_TSL_Dienst auf (vgl. A_17661).

(13) none.[248]

FDP_ACF.1.3/AK.TLS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[249].

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.

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

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

(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_VSDD_Fachdienst, S_KSR oder S_Verzeichnisdienst (VZD) die OCSP-Antwort

(a) CERT_REVOKED, oder

(b) CERT_UNKNOWN, oder

(c) OCSP_CHECK_REVOCATION_FAILED

lautet, so muss der EVG den Verbindungsaufbau abbrechen[250].

(6) Falls bem Aufbau der Verbindung zu S_TSL_Dienst die Prüfung des Zertifkats des S_TSL_Dienst gemäß TUC_KON_037 fehlschlägt oder andere Fehler beim Aufbau der TLS-Verbindung auftreten MUSS der EVG den Verbindungsaufbau gemäß A_17661 abbrechen.

Anwendungshinweis 178: Für den Fall, dass durch die Konfiguration *ANCL_TLS_MANDATORY=Disabled* eine erzwungene Authentisierung der Clientsysteme abgeschaltet wurde, ist durch eine Klarstellung im Benutzerhandbuch dafür gesorgt, dass der Nutzer über diesen Systemzustand und dessen Folgen informiert ist. [*86*] 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.

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

Anwendungshinweis 179: Der Konnektor muss beim TLS-Verbindungsaufbau den OCSP-Status des TLS-Serverzertifikates gemäß TIP1-A_7254 [93] 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[251] to restrict the ability to ~~change_default~~, query, modify, ~~delete~~, no other operation[252] the security attributes ***Authentisierungsmechanismus***[253] to S_Administrator. **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_TLS_MANDATORY [93]. Die Zuweisung anderer Operationen kann leer bleiben.

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 to provide *restrictive*[254] 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[255] 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.

[251] [assignment: *access control SFP(s), information flow control SFP(s)*]

[252] [assignment: other operations]

[253] [assignment:, *list of* ***additional*** *security attributes*]

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

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

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 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.

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 Authentisisierung 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**
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 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“.

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 Siehe FTP_ITC.1/NK.KSR in Abschnitt 6.2.6.

Anwendungshinweis 183: Die Verfeinerung des Elementes FTP_ITC.1/NK.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 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 BNetzA-VL Hashwerts, Download der BNetzA-VL und Download der Hash-Datei der TSL(ECC-RSA).

Anwendungshinweis 184: Die Verfeinerung des Elementes FTP_ITC.1/AK.TSL 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.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** ~~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 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* **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. [92], 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.**
FTP_ITC.1.2/AK.eHKT	The TSF shall permit another trusted IT product **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.

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 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.

Operation	Beschreibung	Anmerkung
Lesen	Für den Zugriff auf den Inhalt des sicheren (geschützten) Datenspeichers durch den Konnektor ist die Nutzung des Schlüsselmaterials erforderlich. Dazu muss dieser gelesen werden können.	Der sichere Datenspeicher muss während der gesamten Betriebszeit des Konnektors zur Verfügung 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 24: Operationen zum Zugriff auf den sicheren Datenspeicher

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 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.

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,

(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 „Administratorobjekt“ darf nur innerhalb einer Administratorsitzung entschlüsselt und gelesen und verschlüsselt und geschrieben werden, aber nicht außerhalb der Administratorsitzung gespeichert werden,

(5) none.[256]

FDP_ACF.1.3/AK.SDS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[257].

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) none.[258]

Anwendungshinweis 187: Der sichere Datenspeicher kann in Form einer transparenten Speicherverschlüsselung (Containerverschlüsselung) realisiert werden. Temporär gespeicherte Datenobjekte aus dem sicheren Datenspeicher dürfen im abgeschalteten Zustand des Konnektors nicht zugänglich sein. Für den Zugriff auf die dazu nötigen Schlüssel kann die gSMC-K (als Speicherort) ggf. in Verbindung mit einer SMC-B oder einem HBA (zur Autorisierung des Zugriffs) verwendet werden.

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

257 257[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

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

Anwendungshinweis 188: Der Netzkonnektor stellt ein symmetrisch verschlüsseltes Filesystem (Crypted File System, CFS) als Datenspeicher für sichere Speicherung von Geheimnissen zur Verfügung. Der symmetrische Schlüssel selbst wird durch einen asymmetrischen Schlüssel, der in der gSMC-K („sicherer Schlüsselspeicher“) hinterlegt ist, geschützt. Dieser Speicherbereich wird beim ersten Start nach der Auslieferung des Konnektors gemäß den Beschreibungen in den Herstellerdokumenten zum Aspekt ADV_ARC initialisiert.

Anwendungshinweis 189: Die vorliegenden Sicherheitsvorgaben sehen keine Datenobjekte mit dem Sicherheitsattribut „Administratorobjekt“ vor. Daher sind die Zugriffsbeschränkungen auf solche Objekte aus der SDS-SFP tautologisch.

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 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; objects: (1) Daten der Chipkarten (Versichertenstammdaten), (2) Objektsystem der Chipkarte (eGK); operations: (1) Lesen der Versichertenstammdaten, (2) Schreiben der Versichertenstammdaten, (3) Ergänzen des Objektsystems.

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 Modifi-zieren der Versicherten-stammdaten der eGK	Diese Operation kann die Kartenkommandos SELECT, ERASE BINARY, , UPDATE BINARY, WRITE BINARY, 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 25: Operationen zum Zugriff auf die eGK 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 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).
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 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[259].

FDP_ACF.1.3/AK.VSDM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[260].
FDP_ACF.1.4/AK.VSDM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[261].

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 to restrict the ability to ***create,*** *query, modify, no other operation*[262] the security attributes none[263] to S_Administrator.
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 to provide restrictive 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 to specify alternative initial values to override the default values when an object or information is created.

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

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

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

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

263 [assignment: list of security attributes]

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.

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 „Ordnungsgemäßigkeit der Signatur“ verschlüsselter Daten nur dann auf „ordnungsgemäß“, wenn

(a) die identifizierte Verschlüsselungsrichtlinie für die zu verschlüsselnden Daten 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

(d) keine Fehler auftraten.

Anwendungshinweis 191: Die Zuweisung in der Regel (5) muss in Übereinstimmung mit den Zugriffsregeln der qualifizierten Signaturerstellungseinheit erfolgen. Für die Stapelsignatur nach TR-03114 [75] 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,
- 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 [75], 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 wird dies wie ein vom Benutzer geforderter Abbruch der PIN-Eingabe behandelt, siehe [93], TAB_KON_752.
- Die SFR FMT_MSA.4/AK erfasst die von BSI-CC-PP-0098-V3 vorgesehenen Signaturarten ergänzt um die Komfortsignatur. Im Fall der Komfortsignatur entfällt die Regel (6)f in FMT_MSA.4.1/AK als zu erfüllende Bedingung.

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 the following objects: (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. **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 sensitive Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. wenn möglich vor Reset, überschrieben werden.**

Anwendungshinweis 192: Beim Ziehen einer Chipkarte sowie beim Entfernen eines Kartenterminals werden eventuell vorhandene Objekte nach (1)-(8) in FDP_RIP.1/AK, die evtl. im Puffer (Cache) vorhanden sind, 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.
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.
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 disable and enable the functions Online Kommunikation, Signaturdienst und Logische Trennung to Administrator. **The following rules apply:** **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/NK.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: The TOE implements MGM_LOGICAL_SEPARATION="Disabled", and this cannot be changed. Therefore, this rule does not apply here.[264]**

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 VPN-Client, vergl. FMT_MSA.1/NK. Im vorliegenden EVG gilt außerdem unveränderlich MGM_LOGIGAL_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

[264] Klarstellung, dass die Regeln für MGM_LOGICAL_SEPARATION=Enable aus BSI-CC-PP-0098-V3 hier unberücksichtigt bleiben.

(1) set, query, modify and delete the roles from other users,

(2) set, modify and delete the authentication credentials for administrators,

(3) set and modify the Arbeitsplatzkonfiguration with assigned Clientsystem and eHealth-Kartenterminals,

(4) set and modify the Zeitpunkten und Gültigkeitsdauer der Prüfungsergebnisse zur Gültigkeit qualifizierter Zertifikate für die Erzeugung ordnungsgemäßer qualifizierten elektronischen Signaturen,

(5) change_default of the gültigen Signaturrichtlinie für Signaturerzeugung,

(6) change_default of the gültigen Signaturrichtlinie für Signaturprüfung,

(7) modify the configuration paramater to activate or deactivate the automatic installation of software updates,

(8) import the update data for Karten-Terminals and execute the update,

(9) configure the loggable system events,

(10) export and import the configuration data of the TOE,

(11) set and modify the maximum lifetime of OCSP cache entries

(12) set and modify the keys of the sicheren Datenspeichers,

(13) set and import the X.509 certificates of Clientsystemen,

(14) reset to factory settings of ~~the~~ all TSF data (factory reset),

(15) import the CA certificates of an encryption PKI

(16) change default and set the SAK_COMFORT_SIGNATURE

(17) change default and set the SAK_COMFORT_SIGNATURE_MAX

(18) change default and set the SAK_COMFORT_SIGNATURE_TIMER

to administrator.

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 Clientsystemen (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). Der Defaultwerte von SAK_COMFORT_SIGNATURE muss auf „disabled" stehen, die Defaultwerte für SAK_COMFORT_SIGNATURE_MAX und SAK_COMFORT_SIGNATURE_TIME muss gem. TIP1-A_4680-03 in [93] gesetz sein. Dabei darf SAK_COMFORT_SIGNATURE nur dann auf „enabled" gesetzt werden können, wenn gleichzeitig auch ANCL_TLS_MAndatoty und ANCL_CAUT_MANDATORY auf „enabled" gesetzt sind oder werden.

Anwendungshinweis 195: Der EVG bietet Funktionalität für automatische Updates und setzt daher die Regel (7) von FMT_MTD.1/AK.Admin um.

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 the public keys of the CVC root CA to the CMS of the gSMC-K, (2) **import and permanently store the public keys of the CVC root CA by the use of cross CVC to S_AK.**

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.
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, including Hash-Datei der TSL(ECC-RSA) (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) *Signaturrichtlinie und Verschlüsselungsrichtlinie*[265]

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 [100] 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 [79] 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.

(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 Signaturrichtlinie NFDM die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen*[266]

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

265 [Selection: Signaturrichtlinie, Verschlüsselungsrichtlinie]

266 [Auswahl: *für Signaturrichtlinie die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen, für Verschlüsselungsrichtlinie die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Zulässigkeit prüfen, weitere einschränkende Regeln für nicht-qualifizierte elektronische Signaturen*]

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 im Schutzprofil BSI-CC-PP-0098-V3 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. Zur Klarstellung und Abgrenzung des Begriffs Signaturrichtlinie sowie zu einschränkenden Regeln bei der Nutzung der Konnektorschnittstelle zum Signieren sei auf Abschnitt 7.3.5 dieser Sicherheitsvorgaben verwiesen.
Die in der letzten Regel von FPT_TDC.1.2 genannten Signatur- und Verschlüsselungsrichtlinien (zu unterstützende Dokumenten- / Signatur- / Verschlüsselungsformate und XML-Daten-Interpretationsvorschriften) werden im Zuge von Updates des EVG (vorrangig beim Einbringen neuer Fachmodule) importiert. Die Signaturprüfung erfolgt dann im Zuge der Signaturprüfung des Update-Pakets entsprechendFDP_ACF.1/NK.Update.

Anwendungshinweis 197: Die BNetzA-VL muss gemäß Anforderung A_6730 der Konnektor-Spezifikation [92] im Online-Modus mindestens einmal täglich auf Aktualität überprüft werden. Der EVG muss den Hash-Wert der BNetzA-VL gemäß Use Case TUC_KON_031 der Konnektor-Spezifikation [92] interpretieren.

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 [92]** when the following types of failures occur: (1) according to TAB_KON_503 [92] with type „SEC“ and severity „fatal“. (2) none[267]. **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.**

[267] [assignment: list of additional types of failures in the TSF]

Anwendungshinweis 198: Für dedizierte Fehlerarten muss der EVG bestimmte weitere Funktionalität unterbinden. Diese Fehlerarten und die erlaubten bzw. verbotenen Dienste sind in Tabelle TAB_KON_504 in [92] definiert. Darunter ist auch der Fehlerfall EC_FW_Not_Valid_Status_Blocked vom Typ „SEC“. Der Konnektor muss gemäß TIP1-A_6025 in [93] täglich prüfen, ob ein als kritisch gekennzeichnetes SW-Update zur Verfügung steht, das noch nicht installiert worden ist und dessen Deadline überschritten ist. Ist dies der Fall, so muss der Konnektor den kritischen Betriebszustand EC_FW_Not_Valid_Status_Blocked annehmen, den Verbindungsaufbau zur TI-Plattform verhindern sowie bestehende Verbindungen in die TI abbauen. Es gelten weiterhin die Einschränkungen aus TIP1-A_4510-02 [*86*].
Im Fehlerfall EC_Firewall_Not_Reliable deaktiviert der EVG die LAN- und WAN-Schnittstelle. Der Zustand wird durch LEDs am EVG eindeutig signalisiert. Das Handbuch des EVG weist in diesem Fall den Nutzer an, den Support des Herstellers zu kontaktieren. Wenn auch nach einem Reboot (durch Ziehen bzw. Einstecken des Stromkabels) der Fehlerfall fortbesteht, ist der Konnektor nicht mehr einsatzfähig und muss außer Betrieb genommen werden.
Alle weiteren von vorgenannter SFR erfassten Fehlerfälle werden so behandelt wie in TAB_KON_504 [93] festgelegt (Ausnahme: der Fehlerzustand EC_NK_Certificate_Expired wird nicht unterstützt). Gemäß A_17549 [93] muss der EVG den manuellen Import des TSL-Signer-CA Cross-Zertifikats auch ermöglichen, wenn er sich im kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period befindet. Für alle weiteren von vorgenannter SFR erfassten Fehlerfälle gelten die in TAB_KON_504 [82] festgelegten Verbote. Die aktuelle Implementierung nimmt auch auf die beiden Zustände EC_CRL_OUT_OF_DATE und EC_TSL_TRUST_ANCHOR_OUT_OF_DATE Rücksicht. In diesen Zuständen ist keine Verbindung zur TI und zum SIS möglich.

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[268] 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. **(2) bei der Meldung eines eHealth-Kartenterminals über das**

[268] [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

Stecken einer Chipkarte 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.

(3) bei entfernter Eingabe von PIN- oder PUK 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 CVC Flag '55' für die Nutzung einer Chipkarte als PIN-Empfänger für die entfernte PIN-Eingabe.

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 TUC_KON_256 aus [93] mit CardType=UNKNOWN ausführen[269].

Anwendungshinweis 200: Die offene Operation im Element FPT_TEE.1.2 wurde entsprechend der Unterstützung weiterer Chipkarten ausgeführt, denn es werden keine weiteren Chipkarten unterstützt. Der genannte Use Case erstellt eine Systemereignismeldung des Typ „Op" und des Schweregrades „Info". 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. [94]). 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.

[269] [assignment: action for unknown smart cards]

FPT_TST.1.1/AK.Run-Time	The TSF shall run a suite of self tests beim Anlauf und regelmäßig während des Normalbetriebs[270] to demonstrate the correct operation of parts of TSF: (1) Signaturprüfung der Images, die ausführbaren Code enthalten (Host-OS, alle VMs), (2) Known-Answer-Tests des Zertifikatsdienstes, (3) Known-Answer-Test des Moduls OpenSSL[271].
FPT_TST.1.2/AK.Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of parts of TSF data: (1) Öffentlicher Schlüssel zur Prüfung der BNetzA-VL, (2) Öffentlicher Schlüssel zur Prüfung von TSL, (3) Öffentlicher Schlüssel zur Prüfung der XML-Signatur der BNetzA-VL, (4) Öffentlicher Schlüssel der Sub-CA der Verschlüsselungszertifikate, (5) Öffentlicher Schlüssel der Wurzelinstanz der CVC, (6) Vergleich von C.AK.AUT zwischen gSMC-K und Speicher[272].
FPT_TST.1.3/AK.Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of [same parts of TSF] as in FPT_TST.1.1/AK.Run-Time[273].

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. Typische Testmethoden beim Anlauf sind z. B. Known-Answer-Tests komplexer Sicherheitsfunktionen. Typische Testmethoden während des Normalbetriebs sind z. B. Kontrollberechnungen wie die Überprüfung des symmetrischen Verschlüsselns durch Entschlüsseln und Vergleich des ursprünglichen und des aus dem Geheimtext entschlüsselten Klartextes. Die Verfeinerungen der Elemente FPT_TST.1/AK.Run-Time sind zur Präzisierung in den vorliegenden Sicherheitsvorgaben genutzt worden. Details zu den Selbsttests sind [RISE-KON-ITD] zu entnehmen.

FPT_TST.1/AK.Out-Of-Band	**TSF testing / Out-Of-Band**

[270] [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]*]

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

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

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

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 to demonstrate the correct operation of TSF.
FPT_TST.1.2/AK.Out-Of-Band	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
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[274].

Anwendungshinweis 202: Das Element FPT_TST.1.1/Out-Of-Band fordert ergänzend zu FPT_TST.1/Run-Time einen Selbsttest des EVG beim Erstanlauf und auf Anforderung eines autorisierten Benutzers, der außerhalb der normalen Betriebsbedingungen, d. h. bei dem Erstanlauf nach der Installation oder in einem gesonderten Testbetrieb, erfolgen kann. Das Element FPT_TST.1.3/Out-Of-Band fordert den Code der prüfenden TSF-Komponenten vor unerkannten Veränderungen integritätsgeschützt zu speichern und vor Veränderungen durch Funktionsstörungen oder Angriffe zu schützten. Die vorliegenden Sicherheitsvorgaben berücksichtigen keine solchen Tests. Dies ist dadurch gerechtfertigt, dass im Rahmen des Secure Boot (vgl. auch Abschnitt 7.1.5) bereits auf Basis eines im BIOS hinterlegten Sicherheitsankers eine Integritätsprüfung der gesamten TSF stattfindet.

FPT_STM.1/AK	**Reliable time stamps**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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

[274] [assignment: parts of TSF mit gespeichertem ausführbarem TSF-Code]

der Selbstschutz, die Domain-Separierung und die Nichtumgehbarkeit der Sicherheitsfunktionalität realisiert ist [3].

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*[275] 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, Software-Updates durchzuführen*[276]**,** • *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*[277]
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

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

[276] Dieser Zusatz weicht von BSI-CC-PP-0098-V3 ab und stellt klar, welche Versuche vom SFR erfasst sind.

[277] *[assignment: additional events]*

b) For each **specified** audit event type, based on the auditable event definitions of the functional components included in the PP/ST, none[278].

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.

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. Zum Nachweis dieser Anforderung für die Produktzulassung sind alle möglichen Protokoll-Einträge zu dokumentieren. Die Spezifikation Konnektor [92] 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 administrators[279] with the capability to read the auditable events according to FAU_GEN.1/AK[280] 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 unauthorised modifications to the stored audit records in the audit trail.

278 [assignment: *other audit relevant information*]

279 [assignment: *authorised users*]

280 [assignment: *list of audit information*]

Anwendungshinweis 204: Nach [92] ist kein Nutzer befugt, Modifizierungen der Protokollaufzeichnungen vorzunehmen. Der Protokollspeicher muss mindestens 250 Einträge aufnehmen können und ältere Einträge ggf. rollierend überschreiben.

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 and switch to the state EC_LOG_OVERFLOW according to TAB_KON_504 [92] [281] if the audit trail is full.

6.3.7. VAU-Kommunikation

Die folgenden SFR wurden in dieses Security Target aufgenommen, um sicher zu stellen, dass die kryptographischen Sicherheitsanforderungen an die im Konnektor zu nutzende VAU-Kommunikation im Rahmen des Zugriffs auf die elektronische Patientenakte evaluiert werden.

Hinweis 1: Das VAU-Protokoll wird innerhalb eines gesicherten TLS-Kanals zwischen dem Konnektor und der Telematikinfrastruktur verwendet. Das VAU-Protokoll schützt die Kommunikationsstrecke zwischen dem Fachmodul ePA und der VAU.

FTP_ITC.1/VAU	**Inter-TSF trusted channel**
	Grundlegende Sicherheitsleistungen des VAU-Protokolls
Dependencies:	No dependencies.
FTP_ITC.1.1/VAU	The TSF shall provide a communication channel between itself and 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**[282] disclosure.
FTP_ITC.1.2/VAU	The TSF **must be able to**[283] permit *the Fachmodul ePA* [284] to initiate communication via the trusted channel.

[281] [assignment: other actions to be taken in case of audit storage failure]

[282] refinement (or → and)

[283] refinement (shall → must be able to)

[284] [selection: *the Fachmodul ePA]*

FTP_ITC.1.3/VAU The TSF shall initiate communication via the trusted channel for *communication required by the Fachmodul ePA]*[285].

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von unbefugtem Löschen, Einfügen oder Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss auf Basis des VAU-Protokolls aufgebaut werden (siehe gemSPec_Krypt [87] insb. A_16883 und A_15549[286]). Dabei muss folgende Chiper Suite verwendet werden:

AES-256-GCM-BrainpoolP256r1-SHA-256

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. Dazu mussdie Client beim Empfang der VAUServerHelloData-Nachricht die Authentizität und Integrität des zur Signatur der im Feld „Data“ enthaltenen Daten unter Verwendung der TSL der Telematikinfratsurktur prüfen und muss den Protokollablauf abbrechen, wenn die Prüfung fehlschlägt. (vgl. [87] A_16941) oder das Zertifikat der VAU nicht die Rolle oid_epa_vau hat. Ebenfalls muss der Protokollablauf vom EVG abgebrochen werden, wenn der Inhalt des Feldes „Data“ vom Erwartunsgwert abweicht (vgl. [87] A_16903)

Das Fachmodul 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 (vgl. [87] A_17225).

Der EVG muss Nachrichten an den VAU-Server ausschließlich mit den Content-Types ‚application/json‘ und ‚application/octet-stream‘ übermitteln (vgl. [87] A_16884 und A_17071) und darf keine anderen als die ihm bekannten Key-Value-Paare interpretieren (vgl. [87] A_17074).

Zur Signatur von Nachrichten im VAU-Protokoll muss der EVG Schlüsselmaterial verwenden, dass dediziert für die Entity-Authentication vorgesehen ist (AUT-Schlüsselmaterial (einer eGK, einer SMC-B etc.))(vgl. [87] A_17081)

---

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

286 Der Mechanismus, dass eine Neuaushandlung eines AES-Sitzungsschlüssels für die Verbindung zur VAU inkl. Löschung des alten Schlüssels nach spätestens 24 Stunden zu erfolgen hat, wird durch das FM ePA ausgelöst.

Nachrichten vom Typ VAUClientSigFin müssen den Anforderungen aus A_17070 [87] entsprechen und entsprechend A_17071 [87] als Antwort auf eine Nachricht vom Typ VAUServerHello gesendet werden.

Beim Empfang einer VAUServerFin-Nachricht muss der EVG prüfen, ob der Wert im Feld „FinishedData“ dem nach A_16899 [87] zu erwartenden Wert entspricht. Falls nein, muss der EVG den weiteren Protokollablauf abbrechen (vgl. [87] A_17084).

Beim Empfang einer VAUServerError-Nachricht gem. A_16851 muss der EVG dessen Signatur prüfen. Fällt die Prüfung positiv aus, so muss der EVG die Protokollausführung abbrechen ([87] A_16900).

FPT_TDC.1/VAU Inter-TSF basic TSF data consistency

Prüfung der Authentizität und Integrität der zur Signatur von Daten verwendeten Schlüssel

Dependencies: No dependencies.

FPT_TDC.1.1/VAU The TSF shall provide the capability to consistently interpret

(1) *eine Liste gültiger öffentlicher Schlüssel zur Verwendung durch Server im VAU-Protokoll (Trust-Service Status List TSL)*

(2) *Von VAU-Servern präsentierte Zertifikate (Prüfung gem. A_17225)*

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/VAU The TSF shall use *interpretation rules*[287] when interpreting the TSF data from another trusted IT product.

Refinement: Die „interpretation rules“ umfassen: Der EVG muss prüfen können, ob der für eine Signatur der Daten in der Nachricht VAUServerHelloData verwendete private Schlüssel zu dem in der TSL der Telematikinfrastruktur hinterlegten öffentlichen Schlüssel der VAU-Server-Komponente gehört und ob die gebildete Signatur mathematisch korrekt ist. Der EVG muss den Protokollablauf abbrechen, wenn die Prüfung fehlschlägt. (vgl. [80] A_16941).

Hinweis: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [93] 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 [93]).

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

Die nachfolgende SFR setzt die Anforderungen A_16852-01 und A_16943-01 aus [87] um.

FCS_CKM.1/VAU Cryptographic key generation / VAU

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

hier erfüllt durch: FCS_COP.1/VAU

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 *ECDH gemäß [68], für HKDF: Ableitungsvektor AES-256-GCM-Key*[288] and specified cryptographic key sizes *256 bit for AES-256*[289] that meet the following: *Standard RFC 5869 [69]*[290]

Hinweis: Für den Elliptic-Curve-Diffie-Hellman-Keyexchange werden die gemäß [87] vorgegebenen Kurven unterstützt.

FCS_COP.1/VAU Cryptographic operation

Zu unterstützende Verschlüsselungs-Algorithmen für das VAU-Protokoll in FTP_ITC.1/VAU

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 The TSF shall perform *symmetric authenticated encryption and decryption*[291] in accordance with a specified cryptographic algorithm *AES-256 in GCM Mode*[292] and cryptographic key sizes *256 bit*[293] that

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

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

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

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

[292] [assignment: *cryptographic algorithm*]

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

meet the following: *RFC 5289 [61], specification [87]* [294]*(, A_16945, A_16957, A_17069, A_18004).*

6.3.8. SGD-Kommunikation

Die folgenden SFR wurden in dieses Security Target aufgenommen, um sicherzustellen, dass die kryptographischen Sicherheitsanforderungen an die im Konnektor zu nutzende SGD-Kommunikation evaluiert werden.

Hinweis 1: Die Kommunikation zwischen dem FM ePA des Konnektors und dem SGD erfolgt – wie jede Kommunikation zwischen Konnektor und TI - innerhalb eines IPSec-Tunnels zwischen Konnektor und VPN-Zugangsdienst.

Hinweis 2: Zwischen Anwendungskonnektor und der Requestverarbeitenden Einheit des SGD (SGD-RVE) wird eine einseitig authentisierter TLS-Verbindung hergestellt. Dazu werden die in Abschnitt 6.2.8 dargestellten SFR (insb. FTP_ITC.1/AK.FD) für TLS-Verbindungen mit der Einschränkung, dass lediglich eine Authentisierung der SGD-RVE stattfindet, verwendet. Die SFR werden hier nicht nochmals dargestellt.

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

Prüfung der Gültigkeit von TLS-Zertifikaten eines SGD-HSM

Dependencies: No dependencies.

FPT_TDC.1.1/SGD.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*

when shared between the TSF and **einem SGD-HSM**

FPT_TDC.1.2/SGD.Zert The TSF shall use *interpretation rules*[295] when interpreting the TSF data from **eines SGD-HSM**.

Refinement: Die „interpretation rules“ umfassen: Der EVG muss prüfen können, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und anhand der TSL prüfen, ob ein Zertifikat in einer Whitelist enthalten ist.

Darüber hinaus muss bei Prüfung eines SGD-HSM-Zertifikats bei bzw. vor der Erzeugung eines Requests an den SGD prüfen, ob das Zertifikat in der TSL innerhalb eines "TSPService"-Eintrags mit

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

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

dem ServiceTypeIdentifier "http://uri.etsi.org/TrstSvc/Svctype/unspecified" aufgeführt ist und dieses zeitlich aktuell gültig ist. Falls nein, so MUSS das Zertifikat abgelehnt werden und die Verarbeitung des Zertifikats abgebrochen werden (vgl- A_17847 in [99]).

Weiterhin muss, falls bei der Prüfung eines SGD-HSM-Zertifikats ein SGD-1-Zertifikat erwartet wird, geprüft werden, ob die OID oid_sgd1_hsm im SGD-HSM-Zertifikat (Kontext Prüfung der Signatur der aktuellen SGD-HSM-ECIES-Schlüssel) aufgeführt ist (und entsprechend oid_sgd2_hsm im Fall eines SGD2-Zertifikats). Falls nicht, so MUSS das Zertifikat abgelehnt werden (vgl- A_17848 in [99]).

Hinweis: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [93] 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 [93]).

FTP_ITC.1/SGD Inter-TSF trusted channel

Grundlegende Sicherheitsleistungen des Datenkanals zwischen dem EVG und dem SGD-HSM

Dependencies: No dependencies.

FTP_ITC.1.1/SGD The TSF shall provide a communication channel between itself and **a SGD-HSM** 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**[296] disclosure.

FTP_ITC.1.2/SGD The TSF **must be able to**[297] permit *the Fachmodul ePA* [298] 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 Fachmodul ePA]*[299].

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.

296 refinement (or → and)

297 refinement (shall → must be able to)

298 [selection: *the Fachmodul ePA]*

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

Die Anforderung „assured identification" im ersten Element des SFR impliziert, dass der EVG in der Lage sein muss, die Authentizität des „SGD-HSM" zu prüfen.

Der EVG muss zur Sicherung des Datenkanals das ECIES-Verfahren verwenden. Zu Beginn des Kanalaufbaus muss der EVG den zum Abfragezeitpunkt gültigen, öffentlichen SGD-HSM-ECIES-Schlüssel mit der Operation GetPublicKey sowohl von SGD1 als auch von SGD2 abrufen (vgl. A_17897 in [87]) und deren zugehörige Signature gemäß A_18024 und A_19971 [87] prüfen. Im Fall einer negativen Prüfung muss die Kommunikation abgebrochen werden.

Im Fall einer positiv verlaufenden Prüfung muss der EVG ein eigenes kurzlebiges ECIES-Schlüsselpaar erzeugen (vgl. (A_18032, A_17874 und FCS_CKM.1/SGD.ECIES). Aus den Hashwerten der abgerufenen öffentlichen ECIES-Schlüssel der SGD1 und SGD2 sowie seinem eigenen öffentlichen ECIES-Schlüssels erzeugt das EVG eine Kodierung gemäß A_17900 in [99] und signiert diese mit der AUT-Identität des Benutzers (vgl- A_17901 in [99]). Im Fall der Nutzung einer eGK / SMC-B der Generation 2.0 muss der eigene ephemeren Schlüssels mit RSASSA-PSS und SHA-256 signiert werden, im Fall der Nutzung von Karten der Generation 2.1 oder höher kommt ausschließlich ECDSA zum Einsatz. Diese Unterscheidung sowie die Auswahl des Signaturverfahrens geschieht in Analogie zu FCS_COP.1/AK.CMS.Sign in Verbindung mit den zugehörigen Anwendungshinweisen.

Unter Verwendung von OE.NK.RNG muss der EVG eine 256-Bit lange Challenge erzeugen und in Hexadezimalform kodieren. Weiterhin MUSS der Client den SHA-256-Wert aus der Aneinanderreihung seines Client-spezifischen ECIES-Schlüssels in der Kodierung nach A_17900 und des für dessen Signatur verwendeten AUT-Zertifikats (DER-kodiert) berechnen. Dieser Hashwert wird hexadezimal kodiert und wird so kodiert als Wert H bezeichnet. Anschließend MUSS der Client die Zeichenkette "Challenge <RND-Client> <Wert-H>" erzeugen (Länge der Zeichenkette: 9+2+2*64 = 139 Zeichen) und mittels des ECIES-Verfahrens verschlüsseln. Das erhaltene Chiffrat MUSS der Client gemäß A_17902 kodieren und die Kodierung als "EncryptedMessage" bei Operation GetAuthenticationToken (A_18201) verwenden.

Der EVG muss die auf GetAuthenticationToken erhaltene Response unter Verwendung des privaten Schlüssels des kurzlebigen ECIES-Schlüsselpaares entschlüsseln und gegen die in A_18028 [99] aufgeführten Kriterien prüfen. Falls eine der Prüfungen fehlschlägt, muss der EVG mit einem Fehler abbrechen und ggf. mit dem Protokollablauf neu starten. Der EVG muss den Authentisierungstoken für die im Protokollablauf folgenden Aufruf

der Operation KeyDerivation (A_17898 und A_17888 in [99]) speichern.

Der EVG erzeugt eine Anfrage zur Schlüsselableitung (KeyDerivation) durch das SGD-HSM und erzeugt unter Verwendung von OE.NK.RNG eine zufällige Request-ID. Die Vorgaben aus A_18029 [99] müssen vom EVG eingehalten werden. Der Request muss vom EVG mittels ECIES für das SGD-HSM verschlüsselt und an das SGD-HSM gesendet werden.

Der EVG entschlüsselt die Antwort des SGD-HSM auf den Request KeyDerivation unter Verwendung des privaten Schlüssels des kurzlebigen ECIES-Schlüsselpaares und muss die in A_18031 und A_20977 [99] vorgeschriebenen Prüfungen durchführen. Schlägt eine der Prüfungen fehl, so muss der EVG die erhaltene Antwort (und insb. die darin enthaltenen Schlüssel) verwerfen.

Der EVG muss beim Empfang einer mittels des ECIES-Verfahren verschlüsselten Nachricht den vom Sender empfangenen, ephemeren ECC-Punkt daraufhin prüfen, ob er auf der gleichen elliptischen Kurve wie der Empfänger-ECC-Punkt liegt (vgl. A_17903 [99]).

Darüber hinaus muss der EVG weitere, nachfolgend genannte, einschränkende Anforderungen der Spezifikation [99] umsetzen. Diese betreffen die Aufwärtskompatibilität von JSON-Request (A_17892), die Kodierung von Nachrichten bzw. Auswertung dieser Kodierung (A_17899 und A_17902), die Syntax von Anfragen an das SGD-HSM (A_17924), das Austauschformat (A_17930) sowie die Telematik ID bzw. die KVNR (A_18003 und A_18006).

FCS_COP.1/SGD.AES Cryptographic operation

Ver- und Entschlüsselung der Akten und Kontextschlüssel (gem A_17872 aus [87] induziert durch TUC_KON_075 und TUC_KON_076 aus [93])

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FDP_ITC.1/SGD

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/AK

FCS_COP.1.1/SGD.AES The TSF shall perform *symmetric authenticated encryption and decryption*[302] in accordance with a specified cryptographic algorithm *AES-256 in GCM Mode*[303] and cryptographic key sizes *256 bit*[304] that meet the following: *FIPS-197 [15], NIST-SP800-38D [17].], specification [87]* [305].

FCS_CKM.1/SGD.ECIES Cryptographic key generation

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

hier erfüllt durch: FCS_COP.1/SGD.ECIES

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/AK

FCS_CKM.1.1/SGD.ECIES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *brainpoolP256r1 [66]*[306]
and specified cryptographic key sizes *256 bit*[307] that meet the following: *Standard RFC 5639 [66], specification A_18032 and A_17874 [87]* [308]

FCS_COP.1/SGD.ECIES Cryptographic operation

Nutzung des kurzlebigen ECIES-Client Schlüsselpaares

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/SGD.ECIES

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/AK

---

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

[303] [assignment: *cryptographic algorithm*]

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

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

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

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

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

FCS_COP.1.1/SGD.ECIES The TSF shall perform *ECIES based encryption and decryption*[309] in accordance with a specified cryptographic algorithm *AES-256 in GCM Mode*[310] and cryptographic key sizes *256 bit*[311] that meet the following: NIST-800-56A [68], *FIPS-197 [15], NIST-SP800-38D [17].], specification A_17875 [87]* [312].

Hinweis 1: Für den Ende-zu-Ende-verschlüsselten Datenaustausch zwischen EVG und SGD-HSM muss das ECIES-Verfahren [68] verwendet werden.

Hinweis 2: Der ECDH-Schlüsselaustausch innerhalb von ECIES zwischen EVG und SGD-HSM muss nach [68] Abschnitt 5.7.1.2 durchgeführt werden.

Hinweis 3: Aus dem gemeinsamen ECDH-Geheimnis muss mit der HKDF nach [69] auf Basis von SHA-256 ein AES-256-Bit-Schlüssel abgeleitet werden. Dieser Schlüssel muss mittels AES-GCM und den fachlichen Vorgaben für AES-GCM aus A_17872 [87] verwendet werden, um den symmetrischen Teil der ECIES-Verschlüsselung authentisiert zu ver- bzw. zu entschlüsseln (vgl. A_17874 und A_17875 aus [87]).

Hinweis 4: Der EVG darf das kurzlebige ECIES-Schlüsselpaar nicht für mehr als eine Nutzung der Schlüsselableitungsfunktionalität ePA, also die parallele Anfrage an SGD 1 und SGD 2, nutzen. Dazu wird pro Anwendungsfall ein SGDSvc Instanc erzeugt und das zugehörige Schlüsselpaar und des SGD Authentication Token in der jeweiligen Instanz gespeichert. Die erzeugte SGDSvc Instanz wird grundsätzlich nur einmalig zur Schlüsselableitung verwendet. Ausnahmen sind a) requestFacilityAuthorization, wo die Instanz für das Ableiten der Aktenschlüssel zum Login und zum Ableiten eines neuen Schlüssels für die Berechtigung verwendet wird und b) wenn der SGD Server einen „transienten“ Fehler meldet.

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

Import des vom SGD-HSM gesendeten Schlüsselmaterials

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

Hier erfüllt durch FDP_ACC.1/SGD.

[FMT_MSA.3 Static attribute initialisation]

hier nicht erfüllt. Begründung: FMT_MSA.3 ist nicht erforderlich, da initial kein Schlüssel vorhanden ist.

FDP_ITC.1.1/SGD The TSF shall enforce the *SGD-SFP*[313] when importing user data, controlled under the SFP, from outside of the TOE.

---

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

[310] [assignment: *cryptographic algorithm*]

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

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

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

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

FDP_ITC.1.3/SGD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

A_18029, A_17888, A_20977 and A_18031 in [99] [315].

FDP_ACC.1/SGD Subset access control

Zugriff auf das vom SGD-HSM gesendete Schlüsselmaterial

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 FM-SGD-SFP[316] on

subject: S_ePA_Fachmodul ,

objects: *Response SGD-HSM*

operations:

(1) Importieren des vom SGD-HSM gesendeten Schlüsselmaterials

(2) *Verwenden des vom SGD-HSM gesendeten Schlüsselmaterials*[317]

FDP_ACF.1/SGD Security attribute based access control

Zugriff auf das vom SGD-HSM gesendete Schlüsselmaterial

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: Es liegen intial keine Schlüssel vor.

FDP_ACF.1.1/SGD The TSF shall enforce the [*SGD-SFP*][318] to objects based on the following:

[*subjects: S_ePA_Fachmodul*

objects: Response SGD-HSM

operations:

315 [assignment: *additional importation control rules*]

316 [assignment: *access control SFP*]

317 [assignment: *list of subjects and objects*]

318 [assignment: *access control SFP*]

(1) Importieren des vom SGD-HSM gesendete Schlüsselmaterials

(2) Verwenden des vom SGD-HSM gesendete Schlüsselmaterials]

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:

[

(1) Anfragen an das SGD-HSM dürfen nur vom Subjekt S_ePA_Fachmodul erzeugt und gesendet werden.

(2) *Antworten des SGD-HSM dürfen nur vom Subjekt S_ePA_Fachmodul empfangen und verarbeitet werden.*][319]

FDP_ACF.1.3/SGD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none][320].

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

[

(1) Kein anderes Subjekt als S_ePA_Fachmodul darf Anfragen an das SGD-HSM senden oder empfangen.][321]

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

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

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

6.4. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit sind dies EAL 3, erweitert um die folgenden Komponenten (konform mit CC Teil 3 [3]) ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.3 und ALC_FLR.2.

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

6.4.1. Aus BSI-CC-PP-0098-V3 übernommene Verfeinerungen

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 [92],**
>
> **(2) der Vertraulichkeit und der Integrität der TSF-Daten (s. TIP1-A_4813 Persistieren der Konfigurationsdaten [92]),**
>
> **(3) vor Entnahme der gSMC-K und Kompromittierung der Kommunikation der gSMC-K mit dem EVG**
>
> **beschreiben.**

6.4.2. 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.**

6.4.3. 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 [92], **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.

6.4.4. 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.

6.4.5. Verfeinerungen hinsichtlich der Fachmodule NFDM,AMTS und ePA

Das Fachmodul VSDM ist gemäß zugrundeliegendem Schutzprofil BSI-CC-PP-0098-V3 Teil des EVG und wurde demzufolge vollständig in den Sicherheitsanforderungen dieser Sicherheitsvorgaben berücksichtigt.

Der RISE Konnektor enthält neben dem Fachmodul VSMD die modular integrierten Fachmodule NFDM (nach [108]), AMTS (nach [109]) und ePA (nach [112]).

Entsprechend der Technischen Richtlinien TR-03154 ([82]), TR-03155 ([83]), Kapitel 3.3.2 bzw. TR-03157 ([84]), Kapitel 3.2.2 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.*

Diese Sicherheitseigenschaften sowie die vom jeweiligen Fachmodul aufgerufenen TUCs nach [93] werden jeweils in Kapitel 3.3.2 der Technischen Richtlinien TR-03154 [82], TR-03155 [83] bzw. TR-03157 ([84]), Kapitel 3.2.2, aufgeführt. Um sicherzustellen, dass im Rahmen der Evaluierung nach Common Criteria diese Sicherheitseigenschaften evaluiert werden, sind die folgenden Anforderungen an die Vertrauenswürdigkeit (Assurance) entsprechend verfeinert:

Für den EVG gelten die folgende Verfeinerungen:

ASE_TSS wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 ([82]), TR-03155 ([83]), Kapitel 3.3.2, bzw. TR-03157 ([84]), Kapitel 3.2.2, werden Anforderungen an den Konnektor gestellt, die im Rahmen der Evaluierung berücksichtigt werden müssen. Die für die Fachmodule NFDM, AMTS und ePA 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 ([82]), TR-03155 ([83]), jeweils Kapitel 3.3.2, bzw. TR-03157 ([84]), Kapitel 3.2.2, relevanten Sicherheitseigenschaften des Konnektors umsetzt.

Der Evaluator muss prüfen, dass die gemäß TR-03154 ([82]) und TR-03155 ([83]), Kapitel 3.3.2, bzw. TR-03157 ([84]), Kapitel 3.2.2 relevanten Sicherheitseigenschaften des Konnektors vollständig im Security Target berücksichtigt sind.

ADV_FSP wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 ([82]), TR-03155 ([83]), Kapitel 3.3.2, bzw. TR-03157 ([84]), Kapitel 3.2.2, werden Anforderungen an den Konnektor gestellt, die im Rahmen der Evaluierung berücksichtigt werden müssen. Die dabei von den Fachmodulen aufgerufenen Schnittstellen des Anwendungskonnektors müssen beschrieben werden.

Der Hersteller muss eine Beschreibung der Schnittstellen des Konnektors 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 Vereinerung von ADV_TDS gefordert.

ADV_TDS wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 ([82]), TR-03155 ([83]), Kapitel 3.3.2, bzw. TR-03157 ([84]), Kapitel 3.2.2 werden Anforderungen an den Konnektor gestellt, die im Rahmen der Evaluierung 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 (z.B. 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

SFR	Abhängig von	Erfüllt durch
FAU_GEN.1/AK	FPT_STM.1 Verläßliche Zeitstempel	Echtzeit wird gemäß OE.Zeitdienst durch die Umgebung bereit gestellt.
FAU_SAR.1/AK	FAU_GEN.1/AK Generierung der Protokolldaten	FAU_GEN.1/AK
FAU_STG.1/AK	FAU_GEN.1/AK Generierung der Protokolldaten	FAU_GEN.1/AK
FAU_STG.4/AK	FAU_STG.1/AK Geschützte Speicherung des Protokolls	FAU_STG.1/AK
FCS_CKM.1/AK.AES	[FCS_CKM.2 Verteilung des kryptographischen Schlüssels oder FCS_COP.1 Kryptographischer Betrieb] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FCS_COP.1/AK.AES FCS_CKM.4/AK
FCS_CKM.4/AK	[[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung]	FCS_CKM.1/AK.AES,
FCS_COP.1/AK.AES	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FCS_CKM.1/AK.AES FCS_CKM.4/AK

SFR	Abhängig von	Erfüllt durch
FCS_COP.1/AK.CMS.Ent	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Enc FCS_CKM.4/AK
FCS_COP.1/AK.MIME.Ent	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Enc FCS_CKM.4/AK
FCS_COP.1/AK.MIME.Ver	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Enc FCS_CKM.4/AK
FCS_COP.1/AK.CMS.Sign	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	Erstellung der digitalen Signatur in den Chipkarten, hier nur Datenformatierung
FCS_COP.1/AK.CMS.SigPr	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig, keine Schlüsselerzeugung und keine Schlüsselvernichtung da Signaturprüfung
FCS_COP.1/AK.CMS.Ver	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FCS_CKM.1/AK.AES FCS_CKM.4/AK, asymmetrische Operationen in den Chipkarten
FCS_COP.1/AK.SHA	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische	FDP_ITC.2/AK.Sig, FCS_COP.1/AK.SHA verwendet keine Schlüssel.

SFR	Abhängig von	Erfüllt durch
	Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	
FCS_COP.1/AK.PDF.Sign	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	Erstellung der digitalen Signatur in den Chipkarten, hier nur Datenformatierung
FCS_COP.1/AK.PDF.SigPr	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig, keine Schlüsselerzeugung und keine Schlüsselvernichtung da Signaturprüfung
FCS_COP.1/AK.SigVer.PSS	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig FCS_CKM.4/AK
FCS_COP.1/AK.SigVer.SSA	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig FCS_CKM.4/AK
FCS_COP.1/AK.SigVer.ECDSA	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig FCS_CKM.4/AK
FCS_COP.1/AK.XML.Ent	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Enc FCS_CKM.4/AK Beachte, die Schlüssel für die asymmetrische Entschlüsselung sind in den Chipkarten implementiert.

SFR	Abhängig von	Erfüllt durch
FCS_COP.1/AK.XML.Sign	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FCS_CKM.4/AK Beachte, die Schlüssel für die Signaturerzeugung sind in den Chipkarten implementiert. Deshalb wird die Abhängigkeit von [FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] hier von der Umgebung (Chipkarte) erfüllt.
FCS_COP.1/AK.XML.SigPr	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig FCS_CKM.4/AK
FCS_COP.1/AK.XML.Ver	[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Enc FCS_CKM.1/AK.AES FCS_CKM.4/AK
FDP_ACC.1/AK.eHKT	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.eHKT
FDP_ACC.1/AK.Enc	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.Enc
FDP_ACC.1/AK.Infomod	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.Infomod
FDP_ACC.1/AK.KD	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.KD
FDP_ACC.1/AK.PIN	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.PIN
FDP_ACC.1/AK.Sgen	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.Sgen
FDP_ACC.1/AK.SigPr	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.SigPr
FDP_ACC.1/AK.TLS	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.TLS
FDP_ACC.1/AK.SDS	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.SDS
FDP_ACC.1/NK.Update	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/NK.Update

SFR	Abhängig von	Erfüllt durch
FDP_ACC.1/AK.VSDM	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.VSDM
FDP_ACF.1/AK.eHKT	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.eHKT Die Sicherheitsattribute der eHealth-Kartenterminals werden durch den Administrator gemäß FMT_MTD.1/AK.Admin und FMT_MTD.1/AK.eHKT_Mod ohne initiale Vorzugswerte festgelegt.
FDP_ACF.1/AK.Enc	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.Enc Die durch FDP_ACF.1/AK.PIN benutzten Sicherheitsattribute werden gemäß FDP_ITC.2/AK.Enc importiert und nicht über initiale Vorzugswerte vergeben.
FDP_ACF.1/AK.Infomod	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.Infomod FMT_MSA.3/AK.Infomod
FDP_ACF.1/AK.KD	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.KD FMT_MSA.3/AK.Sig
FDP_ACF.1/AK.PIN	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.PIN Die durch FDP_ACF.1/PIN benutzten Sicherheitsattribute werden durch die Authentisierung der Chipkarten gemäß FIA_UAU.5 bestimmt und nicht über initiale Vorzugswerte vergeben.
FDP_ACF.1/AK.Sgen	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.Sgen FMT_MSA.3/AK.Sig
FDP_ACF.1/AK.SigPr	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.SigPr Die durch FDP_ACF.1/SigPr benutzten Sicherheitsattribute werden gemäß FDP_ITC.2/Sig importiert und nur teilweise gemäß FMT_MSA.3/AK.Sig vergeben.
FDP_ACF.1/AK.TLS	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.TLS FMT_MSA.3/AK.TLS
FDP_ACF.1/AK.SDS	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.SDS Für die Datenobjekte im sicheren Datenspeicher sind keine Sicherheitsattribute festgelegt. Das Management der Schlüssel ist in FMT_MTD.1/AK.Admin geregelt.

SFR	Abhängig von	Erfüllt durch
FDP_ACF.1/NK.Update	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/NK.Update Es findet keine Initialisierung der Sicherheitsattribute für Update-Pakete (Signatur und zulässige Software-Version) durch den EVG statt.
FDP_ACF.1/AK.VSDM	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.VSDM FMT_MSA.3/AK.VSDM
FDP_DAU.2/AK.QES	FIA_UID.1 Zeitpunkt der Identifikation	FIA_UID.1/AK
FDP_DAU.2/AK.Sig	FIA_UID.1 Zeitpunkt der Identifikation	FIA_UID.1/AK
FDP_DAU.2/AK.Cert	FIA_UID.1 Zeitpunkt der Identifikation	FIA_UID.1/AK
FDP_ETC.2/AK.Enc	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflusskontrolle]	FDP_ACC.1/AK.Enc
FDP_ITC.2/AK.Enc	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder FTP_TRP.1 Vertrauenswürdiger Pfad] FPT_TDC.1 Einfache Inter-TSF TSF-Datenkonsistenz	FDP_ACC.1/AK.Enc FPT_TDC.1/AK (in Bezug auf Verschlüsselungszertifkate vorgesehener Empfänger) Das importierte Sicherheitsattribut „Verschlüsselungsrichtlinie“ wird innerhalb des Konnektors von S_AK übergeben. Deshalb ist kein FTP_ITC.1 bzw. FTP_TRP.1 notwendig.
FDP_ITC.2/AK.Sig	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder FTP_TRP.1 Vertrauenswürdiger Pfad] FPT_TDC.1 Einfache Inter-TSF TSF-Datenkonsistenz	FDP_ACC.1/AK.Sgen FDP_ACC.1/AK.SigPr FPT_TDC.1/AK Für FDP_ACF.1/Sgen werden die importierten Sicherheitsattribute „Signaturrichtlinie“ gegen fest implementierte Regeln auf ihre Zulässigkeit geprüft. Für FDP_ACF.1/SigPr sind die importierten Sicherheitsattribute durch geprüfte digitale Signaturen gesichert bzw. die importierten Sicherheitsattribute „Signaturrichtlinie“ wie in FDP_ITC.2/AK.Sig selbst beschrieben gegen fest implementierte Regeln auf ihre Zulässigkeit geprüft. FTP_ITC.1 bzw. FTP_TRP.1 werden deahalb nicht benötigt.
FDP_RIP.1/AK	Keine Abhängigkeiten	-
FDP_SDI.2/AK	Keine Abhängigkeiten	-

SFR	Abhängig von	Erfüllt durch
FDP_UCT.1/AK.TLS	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder FTP_TRP.1 Vertrauenswürdiger Pfad]	FDP_ACC.1/AK.eHKT, FTP_ITC.1/AK.eHKT
FDP_UIT.1/AK.TLS	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder FTP_TRP.1 Vertrauenswürdiger Pfad]	FDP_ACC.1/AK.eHKT, FTP_ITC.1/AK.eHKT
FDP_UIT.1/NK.Update	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder FTP_TRP.1 Vertrauenswürdiger Pfad]	FDP_ACC.1/NK.Update, FTP_ITC.1/AK.TSL, FTP_ITC.1/AK.KSR, FTP_TRP.1/NK.Admin
FIA_API.1/AK	Keine Abhängigkeiten	-
FIA_SOS.1/AK.Passwörter	Keine Abhängigkeiten	-
FIA_SOS.2/AK.Jobnummer	Keine Abhängigkeiten	-
FIA_SOS.2/AK.PairG	Keine Abhängigkeiten	-
FIA_UAU.1/AK	FIA_UID.1 Zeitpunkt der Identifikation	FIA_UID.1/AK
FIA_UAU.5/AK	Keine Abhängigkeiten	-
FIA_UID.1/AK	Keine Abhängigkeiten	-
FMT_MSA.1/AK.Infomod	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen.	FDP_ACC.1/AK.Infomod FMT_SMR.1/AK FMT_SMF.1/AK
FMT_MSA.1/AK.User	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen.	FDP_ACC.1/AK.Sgen FDP_ACC.1/AK.SigPr FMT_SMR.1/AK FMT_SMF.1/AK
FMT_MSA.1/AK.TLS	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen.	FDP_ACC.1/AK.TLS FMT_SMR.1/AK FMT_SMF.1/AK

SFR	Abhängig von	Erfüllt durch
FMT_MSA.1/AK.VSDM	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle] FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen.	FDP_ACC.1/AK.VSDM FMT_SMR.1/AK FMT_SMF.1/AK
FMT_MSA.3/AK.VSDM	FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	FMT_MSA.1/AK.VSDM FMT_SMR.1/AK
FMT_MSA.3/AK.Infomod	FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	FMT_MSA.1/AK.Infomod FMT_SMR.1/AK
FMT_MSA.3/AK.Sig	FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	FMT_MSA.1/AK.User (s. Auswahl der gültigen Signaturrichtlinie), FMT_SMR.1/AK
FMT_MSA.3/AK.TLS	FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	FMT_MSA.1/AK.TLS FMT_SMR.1/AK
FMT_MSA.4/AK	[FDP_ACC.1 Teilweise Zugriffskontrolle, oder FDP_IFC.1 Teilweise Informationsflußkontrolle]	FDP_ACC.1/AK.Sgen FDP_ACC.1/AK.SigPr FDP_ACC.1/AK.Enc
FMT_MOF.1/AK	FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen	FMT_SMR.1/AK FMT_SMF.1/AK
FMT_MTD.1/AK.Admin	FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen	FMT_SMR.1/AK, FMT_SMF.1/AK
FMT_MTD.1/AK.Zert	FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen	FMT_SMR.1/AK FMT_SMF.1/AK
FMT_MTD.1/AK.eHKT_Abf	FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen	FMT_SMR.1/AK, FMT_SMF.1/AK
FMT_MTD.1/AK.eHKT_Mod	FMT_SMR.1 Sicherheitsrollen FMT_SMF.1 Spezifizierung der Managementfunktionen	FMT_SMR.1/AK, FMT_SMF.1/AK
FMT_SMF.1/AK	Keine Abhängigkeiten	-
FMT_SMR.1/AK	FIA_UID.1 Zeitpunkt der Identifikation	FIA_UID.1/AK
FPT_STM.1/AK	Keine Abhängigkeiten	-
FPT_FLS.1/AK	Keine Abhängigkeiten	-
FPT_TDC.1/AK	Keine Abhängigkeiten	-
FPT_TEE.1/AK	Keine Abhängigkeiten	-
FPT_TST.1/AK.Out-Of-Band	Keine Abhängigkeiten	-

SFR	Abhängig von	Erfüllt durch
FPT_TST.1/AK.Run-Time	Keine Abhängigkeiten	-
FTA_TAB.1/AK.Jobnummer	Keine Abhängigkeiten	-
FTA_TAB.1/AK.SP	Keine Abhängigkeiten	-
FTP_ITC.1/AK.eHKT	Keine Abhängigkeiten	-
FTP_ITC.1/AK.QSEE	Keine Abhängigkeiten	-
FTP_ITC.1/AK.CS	Keine Abhängigkeiten	-
FTP_ITC.1/AK.FD	Keine Abhängigkeiten	-
FTP_ITC.1/AK.VZD	Keine Abhängigkeiten	-
FTP_ITC.1/AK.KSR	Keine Abhängigkeiten	-
FTP_ITC.1/AK.TSL	Keine Abhängigkeiten	-

Tabelle 26: Erfüllung der Abhängigkeiten der funktionalen Sicherheitsanforderungen

6.5.3. Erklärung der Abhängigkeiten der funktionalen Sicherheitsanforderungen des VAU-Protokolls

Die Abhängigkeiten für die SFRs des VAU-Protokolls sind bei deren Formulierung in Abschnitt 6.3.7 aufgelöst.

6.5.4. Erklärung der Abhängigkeiten der funktionalen Sicherheitsanforderungen der SGD-Kommunikation

Die Abhängigkeiten für die SFRs des VAU-Protokolls sind bei deren Formulierung in Abschnitt 6.3.8 aufgelöst.

6.5.5. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors durch SFRs des Netzkonnektors

Tabelle 27 stellt die Abbildung der Sicherheitsziele des Netzkonnektors auf Sicherheitsanforderungen des Konnektors zunächst tabellarisch im Überblick dar. In Abschnitt Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors 6.5.7 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_Authenti	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integritä	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

Sicherheitsanforderung an den EVG	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenti	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integritä	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FMT_MSA.3/NK.PF											X	X	
FPT_STM.1/NK					X	X							
FPT_TDC.1/NK.Zert								X					
FDP_RIP.1/NK		X											
FPT_TST.1/NK		X											
FPT_EMS.1/NK		X							X	X			
FAU_GEN.1/NK.SecLog					X								
FAU_GEN.2/NK.SecLog					X								
FMT_SMR.1./NK	X			X							X	X	
FMT_MTD.1/NK				X									
FIA_UID.1/NK.SMR				X									
FTP_TRP.1/NK.Admin	X			X									
FMT_SMF.1/NK	X			X							X	X	
FMT_MSA.1/NK.PF				X							X	X	
FMT_MSA.4/NK				X									
FCS_COP.1/NK.Hash		X								X			
FCS_COP.1/NK.HMAC										X			
FCS_COP.1/NK.Auth			X				X						
FCS_COP.1/NK.ESP									X				
FCS_COP.1/NK.IPsec									X				
FCS_CKM.1/NK		X	X				X		X	X			
FCS_CKM.2/NK.IKE							X		X	X			
FCS_CKM.4/NK	X	X	X				X		X	X			
FTP_ITC.1/NK.TLS	X												
FPT_TDC.1/NK.TLS.Zert	X												
FCS_CKM.1/NK.TLS	X												
FCS_COP.1/NK.TLS.HMAC	X												
FCS_COP.1/NK.TLS.AES	X												
FCS_COP.1/NK.TLS.Auth	X												
FCS_CKM.1/NK.Zert	X												
FDP_ITC.2/NK.TLS	X												
FDP_ETC.2/NK.TLS	X												
FMT_MOF.1/NK.TLS	X												
FDP_ACF.1/AK.TLS	X												

Tabelle 27: Abbildung der EVG-Ziele auf Sicherheitsanforderungen

6.5.6. 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.SignaturVerifizier	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	O.AK.VAU	O.AK:SGD
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																					X	X
FCS_COP.1/AK.AES	X		X				X	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													

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.SignaturVerifizier	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	O.AK.VAU	O.AK:SGD
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.MIME.Ent	X							X																						
FCS_COP.1/AK.MIME.Ver	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																											
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/NK.Update																							X							
FDP_ACC.1/AK.VSDM																											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.SignaturVerifizier	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	O.AK.VAU	O.AK:SGD
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/NK.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														
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/NK.Update																							X							
FIA_API.1/AK													X	X																
FIA_SOS.1/AK.Passwörter		X								X																				
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																

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.SignaturVerifizier	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	O.AK.VAU	O.AK:SGD
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																

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.SignaturVerifizier	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	O.AK.VAU	O.AK:SGD
FTP_ITC.1/AK.CS																			X											
FTP_ITC.1/AK.eHKT			X																											
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							
FTP_ITC.1/VAU																													X	
FPT_TDC.1/VAU																													X	
FCS_CKM.1/VAU																													X	
FCS_COP.1/VAU																													X	
FPT_TDC.1/SGD.Zert																														X
FTP_ITC.1/SGD																														X
FCS_COP.1/SGD.AES																														X
FCS_CKM.1/SGD.ECIES																														X
FCS_COP.1/SGD.ECIES																														X
FDP_ITC.1/SGD																														X
FDP_ACC.1/SGD																														X
FDP_ACF.1/SGD																														X

Tabelle 28: Abdeckung der Sicherheitsziele des EVG durch Sicherheitsanforderungen

6.5.7. 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 29 jedes EVG-Ziel in einzelne Teilaspekte zerlegt, die dann auf Sicherheitsanforderungen abgebildet werden.[322] 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/oder Kursivschrift gekennzeichnet.

Grundsätzlich gilt, dass die korrekte Umsetzung eines Ziel in Sicherheitsanforderungen durch die im CC Teil 2 [2] aufgeführten Abhängigkeiten zwischen funktionalen Sicherheitsanforderungen (SFRs) unterstützt wird: Häufig lässt sich leicht ein SFR finden, welches wesentliche Aspekte des EVG-Ziels umsetzt. Betrachtet man alle Abhängigkeiten, so ergibt sich eine vollständige Abdeckung des EVG-Ziels. In der folgenden Tabelle werden daher abhängige SFRs ebenfalls mit aufgelistet. Dabei wird davon ausgegangen, dass die Abhängigkeit selbst nicht gesondert erläutert werden muss.

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 Gültigkeitsprüfung von Zertifikaten	FCS_CKM.1/NK.Zert FCS_CKM.4/NK FDP_ITC.2/NK.TLS FTP_TRP.1/NK.Admin FDP_ETC.2/NK.TLS FPT_TDC.1/NK.TLS.Zert
	Begründung: Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der EVG das exportieren von X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Managementschnittstelle (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 Managementschnittstelle durch den Administrator importiert	

322 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)
	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 [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [86]“ zugelassen. FCS_COP.1/NK.TLS.Auth die unterstützt die Authentisierung im Rahmen des TLS-Verbindungsaufbaus, indem der dazu zu verwendende Algorithmus spezifiziert wird. FCS_COP.1/NK.TLS.HMAC spezifiziert die HMAC Algorithmen, die im Rahmen des TLS-Verbindungsaufbaus zum Einsatz kommen. Nach erfolgreichem Verbindungsaufbau wird die Kommunikation mit AES gemäß FCS_COP.1/NK.TLS.AES abgesichert. FCS_CKM.1/NK.TLS fordert, dass entsprechendes Schlüsselmaterial generiert wird, FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Schutz	Speicheraufbereitung: temporäre Kopien nicht mehr benötigter Geheimnisse werden unmittelbar nach Gebrauch aktiv überschrieben	FDP_RIP.1/NK
	Begründung: In O.NK.Schutz wird gefordert: „Der EVG löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden.“ Genau dies leistet FDP_RIP.1/NK. Auch die Zuweisung „upon the deallocation of the resource from“ passt zur Forderung in O.NK.Schutz. Die „Geheimnisse (z. B. Schlüssel)“ werden im SFR durch die Zuweisung präzisiert.	
	Selbsttests, Schutz gegen sicherheitstechnische Veränderungen	FPT_TST.1/NK
	Begründung: „Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten:“ → ist als Erläuterung für die Begriffsbildung O.NK.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	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	geheimen Schlüssel verwendet werden. FCS_CKM.1/NK fordert, dass das Schlüsselmaterial (z. B. Integritätsprüfschlüssel) generiert wird. Anmerkung: Alternativ könnte ein Hersteller diese Schlüssel auch importieren; dazu wäre dann zusätzlich FDP_ITC.1 oder FDP_ITC.2 aufzunehmen.	
	Schutz gegen unbefugte Kenntnisnahme (Side Channel-Analysen)	FPT_EMS.1/NK
	Begründung: „Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten." Um den Aspekt „die ihm anvertrauten Benutzerdaten" vollständig abzudecken, wurde die explizite Komponente FPT_EMS.1/NK ergänzt. Dieses SFR fordert genau die Analyse, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen.	
O.NK.Stateful	dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	FDP_IFC.1/NK.PF → FDP_IFF.1/NK.PF
	Begründung: „Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter." Diese Paketfilterung wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF). Die zustandsgesteuerte Filterung wurde in den Operationen und im Refinement zu FDP_IFF.1/NK.PF modelliert.	
O.NK.EVG_Authenticity	Auslieferungsverfahren: Nur authentische EVGs können in Umlauf gebracht werden	FCS_COP.1/NK.Auth FCS_CKM.1/NK FCS_CKM.4/NK
	Begründung: „Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können. Gefälschte EVGs müssen vom VPN-Konzentrator sicher erkannt werden können. Der EVG muss auf Anforderung mit Unterstützung der SM NK einen Nachweis seiner Authentizität ermöglichen." → Die Authentisierung wird mit Kryptoalgorithmen erbracht, die durch FCS_COP.1/NK.Auth spezifiziert werden. FCS_CKM.1/NK fordert eine Generierung des für den Nachweis der Authentizität des EVGs erforderlichen Schlüsselmaterials; FCS_CKM.4/NK unterstützt als abhängige Komponenten dabei.	
O.NK.Admin_EVG	rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen	FMT_MTD.1/NK FMT_SMR.1./NK FMT_SMF.1/NK
	Identifikation / Autorisierung des Administrators	FIA_UID.1/NK.SMR FMT_MSA.4/NK
	sicherer Pfad	FTP_TRP.1/NK.Admin
	Beschränkung der Administration der Firewall-Regeln	FMT_MSA.1/NK.PF
	Begründung: „Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen." → FMT_MTD.1/NK beschränkt den Zugriff wie vom Ziel gefordert auf die Rolle Administrator. FMT_SMR.1./NK modelliert als abhängige Komponente diese Rolle (Administrator). FIA_UID.1/NK.SMR erfordert eine Identifikation des Benutzers vor jeglichem Zugriff auf administrative Funktionalität. Die Menge der administrativen Funktionen wird in FMT_SMF.1/NK aufgelistet.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	„Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung eines Administrators, welcher die lokale Administration des EVG durchführen kann." → Die Authentisierung des Administrators erfolgt durch den EVG selbst. Nach erfolgreicher Authentisierung wird ein Sicherheitsattribut gesetzt. Die dabei anzuwendenden Regeln wurden in FMT_MSA.4/NK modelliert. „Die Administration erfolgt rollenbasiert." → FMT_SMR.1./NK modelliert die Rolle Administrator. „Weil die Administration über Netzverbindungen (lokal über PS2) 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.Admin_Auth	Der Netzkonnektor führt die Authentisierung des Administrators durch.	FMT_SMR.1./NK FTP_TRP.1/NK.Admin FMT_MSA.4/NK FTP_ITC.1/NK.TLS FTP_ITC.1.1/NK.VPN_SIS
	Begründung: FMT_SMR.1./NK modelliert die Rolle des Administrators. FTP_TRP.1/NK.Admin fordert einen sicheren Kommunikationskanal zwischen EVG und Administrator, der ausschließlich über die LAN-Schnittstelle zugreift. Der sichere Kanal wird durch FTP_ITC.1/NK.TLS umgesetzt, in dem ein sicherer TLS-Kanal für lokale Administrierung gefordert wird. Die Kryptografischen Basisdienste werden dabei von O.NK.TLS_Krypto umgesetzt. Für entfernte Administrierung ist zu dem eine VPN Verbindung notwendig, diese wird durch FTP_ITC.1.1/NK.VPN_SIS umgesetzt. Erst nach erfolgreicher Authentisierung wird ein entsprechender Autorisierungsstatus im EVG gesetzt (FMT_MSA.4/NK).	
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.AK.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	Integrität und Authentizität des Software Update durch Administrator	FDP_ACC.1/NK.Update FDP_ACF.1/NK.Update FDP_UIT.1/NK.Update FTP_ITC.1/NK.KSR FTP_TRP.1/NK.Admin FPT_TDC.1/AK FTP_ITC.1/AK.TSL
	Begründung: 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/NK.Update führt die Update-SFP für den Software-Update ein und FDP_ACF.1/NK.Update definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_UIT.1/NK.Update fordert den Empfang der Software-Update-Daten und die Prüfung der Integrität dieser Daten vor dem Update. Die Anforderungen FTP_ITC.1/NK.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 Managementschnittstelle. 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. Die dem Netzkonnektor zugeordnete Update-Funktionalität betreffen nicht das Update der BNetzA-VL, sodass die SFRs FPT_TDC.1/AK und FTP_ITC.1/AK.TSL zur Erfüllung dieses Sicherheitsziels benötigt werden, aber dem Anteil Anwendungskonnektor entnommen sind.	
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 Authentisierung („ … provides assured identification of its end points …“) zu den VPN-Konzentratoren in die Telematikinfrastruktur bzw. ins Internet. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS (IPsec) und FCS_CKM.2/NK.IKE (IKE) legen fest, welche Protokolle im Rahmen des Kanalaufbaus verwendet werden sollen. Zwar geht es in FCS_CKM.2/NK.IKE vorrangig um die Schlüsselableitung, diese ist aber mit der Authentisierung kombiniert. FCS_CKM.1/NK fordert, dass entsprechendes Schlüsselmaterial für die Authentisierung generiert wird (evtl. unter Rückgriff auf eine gSMC-K, welches in den EVG eingebracht wird). FCS_CKM.4/NK unterstützt als abhängige Komponente.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
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-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.	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	FPT_EMS.1/NK sorgt dafür, dass die session keys, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese session keys sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.VPN_Integrität	Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von session keys, Austausch der session keys mit Gegenstelle, Zerstörung der session keys nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von session keys, Zerstörung der session keys nach Verwendung Geheimhaltung der session keys	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Hash →FCS_CKM.1/NK →FCS_CKM.2/NK.IKE →FCS_CKM.4/NK FCS_COP.1/NK.HMAC →FCS_CKM.1/NK →FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht." → Die Integritätssicherung wird durch FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS gefordert („…protection of the channel data from modification and disclosure", man beachte das Refinement von „or" zu „and"). FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Encapsulating Security Payload (ESP) (RFC 4303 (ESP), [52]) 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 ([56], [57], [53]). 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

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Begründung: „Der EVG schützt sich selbst, andere Konnektorteile und die Clientsysteme vor Missbrauch und Manipulation aus dem Transportnetz (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem WAN)." → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects VPN concentrator and attacker communicating with the TOE from its WAN interface (PS3) …" FDP_IFF.1/NK.PF modelliert einen Paketfilter („…the decision shall be based on the following security attributes: IP address, port number, and protocol type.", „For every operation (…) the TOE shall maintain a set of packet filtering rules …"). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (Stateful Packet Inspection) abgebildet und durch ein Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF (für die Paketfilterregeln im Allgemeinen). Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen (z. B Administrator) und verhindert so unbefugte Veränderungen an den sicherheitsrelevanten Filterregeln. FMT_SMR.1./NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf.	
O.NK.PF_LAN	dynamischer Paketfilter zum LAN, regelbasierte Informationsflusskontrolle	FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, FMT_MSA.3/NK.PF, FMT_MSA.1/NK.PF, FMT_SMR.1./NK FMT_SMF.1/NK FDP_IFF.1/NK.PF
	Begründung: „Der EVG schützt sich selbst und den Anwendungskonnektor vor Missbrauch und Manipulation aus möglicherweise kompromittierten lokalen Netzen der Leistungserbringer (dynamische Paketfilter-Funktionalität, Schutz vor Angriffen aus dem LAN)." → Der Schutz wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF): „The TSF shall enforce the packet filtering SFP (PF SFP) on the subjects … and the subjects application connector and workstation (German: Clientsystem) communicating with the TOE from its LAN interface (PS2) …" FDP_IFF.1/NK.PF modelliert einen Paketfilter („…the decision shall be based on the following security attributes: IP address, port number, and protocol type.", „For every operation (…) the TOE shall maintain a set of packet filtering rules …"). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (Stateful Packet Inspection) abgebildet und durch das folgende Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige 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,	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	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 6.4.2.	

Tabelle 29: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 205: Hinweis zu O.NK.VPN_Integrität: Zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash werden nur Hashfunktionen verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruhen, entsprechend sind keine geheimzuhaltenden Schlüssel erforderlich.

6.5.8. Detaillierte Erklärung für die Sicherheitsziele des Anwendungskonnektors

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 [9] für Signaturen und [76] bzw. [*86*] 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 [76].
- FCS_CKM.1/NK.TLS fordert die kryptographische Schlüsselgenerierung von 128 und 256 Bit Schlüsseln gemäß [*86*].
- FCS_CKM.4/AK fordert die Zerstörung von kryptographischen Schlüsseln.
- FCS_COP.1/AK.AES fordert die Verwendung von AES-128 und AES-256 zur symmetrischen Verschlüsselung und 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/AK.MIME.Ent und FCS_COP.1/AK.MIME.Ver fordern die Verwendung des Algorithmus AES-256 für die symmetrische Entschlüsselung und Verschlüsselung von SMIME Daten gemäß [9].
- FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.Auth fordern die Verwendung der Algorithmen 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.

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.

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.

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 [76] 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-Schlüssel gemäß FCS_CKM.1/AK.AES, 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/AK.AES, 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.

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.

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.

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.

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.MIME.Ver die symmetrische Verschlüsselung von SMIME Dokumenten und FCS_COP.1/AK.XML.Ver die symmetrische 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 [76] 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.

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.MIME.Ent die symmetrische Entschlüsselung von SMIME Dokumenten und FCS_COP.1/AK.XML.Ent die symmetrische 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 [76] 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.

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.

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 [76] für die Signaturerstellung zu implementieren.

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 [76] für die Signaturerstellung zu implementieren.

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 Signaturrichtlinien 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.

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.

Das Sicherheitsziel O.AK.Sig.Stapelsignatur “Stapelsignatur“ fordert von dem EVG die Unterstützung der Stapelsignatur gemäß [75]. Die Forderungen aus [75] werden insbesondere durch folgende SFR umgesetzt.

- FIA_API.1 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.

Das Sicherheitsziel O.AK.Sig.Komfortsignatur “Komfortsignatur“ fordert von dem EVG die Unterstützung der Komfortsignatur gemäß [93]:

- FIA_API.1/AK fordert, dass die TSF sich gegenüber der QSEE für die Komfortsignatur authentisiert, und außerdem die Vertraulichkeit und Integrität der Kommunikation per Secure Messaging zu schützen.
- FIA_UAU.5/AK beschreibt die Authentisierung des Clientsystems per UserID vor Ausführung 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 erlangt wurde, nach der Erzeugung einer Signatur im Rahmen einer Komfortsignatur nicht zurückzusetzen, sondern dies nur bei Eintritt der in der SFR genannten Bedingungen zu tun. FDP_ACC.1/AK.Sgen identifiziert die Signaturerstellungs-SFP.
- 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.

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 [76] 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.

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.

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 nicht-qualifizierter 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 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.

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.

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/AK.AES, 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 [33] und [76].
- 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.

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/AK.AES, 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.

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 [77] definiert.

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/NK.Update führt die Update-SFP für den Software-Update ein und FDP_ACF.1/NK.Update definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_UIT.1/NK.Update fordert den Empfang der Software-Update-Daten und die Prüfung der Integrität dieser Daten vor dem Update. Die Anforderungen FTP_ITC.1/NK.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 Managementschnittstelle. 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.

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.

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.

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.

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.

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 die 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.

Das Sicherheitsziel O.AK.VAU „Sicherer, spezifikationskonformer Kanal zur VAU des ePA Aktensystem“ fordert vom EVG die Möglichkeit einer bezüglich Integrität, Authentizität und Vertraulichkeit gesicherten Verbindung zwischen EVG und der VAU des ePA Aktensystems. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- FTP_ITC.1/VAU fordert einen vertrauenswürdigen Kanal zwischen EVG und der VAU des ePA-Aktensystems, dessen Integrität durch FPT_TDC.1/VAU und FCS_COP.1/VAU sichergestellt wird.
- Die Generierung, Nutzung und Zerstörung des ephemeren Schlüsselmaterials wird durch FCS_CKM.1/VAU und FCS_CKM.4/AK abgebildet.

Das Sicherheitsziel O.AK.SGD „Sicherer, spezifikationskonformer Kanal zu den SGD-HSM“ fordert vom EVG die Möglichkeit einer bezüglich Integrität, Authentizität und Vertraulichkeit gesicherten Verbindung zwischen EVG und dem SGD-HSM. Dieses Sicherheitsziel wird durch folgende SFR umgesetzt:

- Die Prüfung der Authentizität des SGD-HSM wird mittels FPT_TDC.1/SGD.Zert modelliert, die Sicherheitsleistungen des SGD-Kanals selbst mittels FTP_ITC.1/SGD.
- Die Ver- bzw. Entschlüsselung des Kontext- bzw. Aktenschlüssels wird mittels FCS_COP.1/SGD.AES und deren sichere Zerstörung mittels FCS_CKM.4/AK abgebildet.

- Die Erzeugung, Nutzung und Zerstörung des ephemeren Schlüsselmaterials für die Kommunikation mit dem SGD-HSM wird mittels FCS_CKM.1/SGD.ECIES, FCS_COP.1/SGD.ECIES und FCS_CKM.4/AK modelliert.
- Der Import der vom SGD-HSM erhaltenen Schlüssel wird mittels FDP_ITC.1/SGD dargestellt. Die Beschränkung der Nutzung des Kanals und des Schlüsselmaterials (user data) wird mittels FDP_ACC.1/SGD und FDP_ACF.1/SGD ausgedrückt.

6.5.9. Erklärung für Erweiterungen

Dieses Security Target definiert keine Erweiterungen, die nicht bereits im BSI-CC-PP-0098-V3 gemacht wurden. Die Erklärung für Erweiterungen aus dem BSI-CC-PP-0098-V3 gilt daher unverändert auch für dieses Security Target.

6.5.10. Erklärung für die Vertrauenswürdigkeitsanforderungen

Dieses Security Target übernimmt die EAL Stufe mit Augmentierung aus dem BSI-CC-PP-0098-V3. Darüber hinaus wird keine weitere Augmentierung vorgenommen. Die Erklärung für Erweiterungen die gewählte EAL-Stufe aus dem BSI-CC-PP-0098-V3 gilt daher unverändert auch für dieses Security Target.

7. Zusammenfassung der EVG Sicherheitsfunktionalität

7.1. Sicherheitsfunktionalitäten des Netzkonnektors

7.1.1. VPN-Client

VPN

Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt. Verbindungen zum *VPN-Konzentrator der Telematikinfrastruktur* werden entsprechend FTP_ITC.1/NK.VPN_TI umgesetzt. Verbindungen zum *Sicheren Internet Service (SIS)* werden entsprechend FTP_ITC.1/NK.VPN_SIS umgesetzt. Der Trusted Channel wird auf Basis des IPsec-Protokolls aufgebaut. Dabei wird IKEv2 unterstützt.

Informationsflusskontrolle

Regelbasiert verwenden 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, verwenden den VPN-Tunnel zum Sicheren Internet Service.

Diese Aspekte ergeben aus der Betrachtung der VPN-Kanäle und werden mittels dynamischen Paketfilters umgesetzt (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, siehe dazu Abschnitt 7.1.2.

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 3.1.1) gefordert, sofern die Paketfilter-Regeln geeignet gesetzt sind.

7.1.2. Dynamischer Paketfilter

Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Der EVG implementiert einen dynamischen Paketfilter. Diese Anforderung wird als Informationsflusskontrolle modelliert (siehe FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF). Zur zustandsgesteuerten Filterung siehe auch Abschnitt 7.1.4.

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).

7.1.3. Netzdienste

Zeitsynchronisation

Bei aktiviertem „Leistungsumfang Online“ (MGM_LU_ONLIONE=Enabled) führt der EVG in regelmäßigen Abständen eine Zeitsynchronisation mit den Zeitservern der Telematikinfrastruktur (die gemäß OE.NK.Zeitsynchro zur Verfügung stehen) durch. Siehe auch Sicherheitsdienst Zeitdienst (siehe FPT_STM.1/NK). Kann eine Zeitsynchronisation innerhalb eines bestimmten Zeitraums nicht erfolgreich durchgeführt werden oder überschreitet

die Zeitabweichung zwischen Systemzeit und Zeit des Zeitservers zum Zeitpunkt der Zeitsynchronisierung einen bestimmten Wert, so wird der kritische Betriebszustand an der Signaleinrichtung des Konnektors angezeigt.

Der Administrator kann die Zeit des Konnektors auch über das Managementinterface einstellen, falls MGM_LU_ONLINE nicht aktiv ist.

Zertifikatsprüfung

Der EVG überprüft die Gültigkeit der Zertifikate, die für den Aufbau der VPN-Kanäle verwendet werden. Die erforderlichen Informationen zur Prüfung der Gerätezertifikate werden dem EVG in Form einer (signierten) Trust-service Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch mittels der aktuell gültigen TSL und CRL (siehe FPT_TDC.1/NK.Zert).

7.1.4. Stateful Packet Inspection

Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“ (engl. „stateful packet inspection“ oder auch „stateful inspection“ genannt). Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird.

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

7.1.5. Selbstschutz

Der EVG schützt sich selbst und die ihm anvertrauten Daten durch zusätzliche Mechanismen, die Manipulationen und Angriffe erschweren. Versuche, den ausführbaren Code zu verändern werden durch Prüfung der Integrität der installierten SW Images bei jedem Start (Secure Boot) gewährleistet (siehe Selbsttests).

Speicheraufbereitung

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

Bei Programmstart wird eine Prüfung der Integrität der installierten ausführbaren Dateien und sonstigen sicherheitsrelevanten Dateien (Konfigurationsdateien, TSF-Daten) durch Verifikation von Signaturen durchgeführt.

Das BIOS unterstützt Secure Boot nach der UEFI Spezifikation [107], Kapitel 30, „Secure Boot and Driver Signing“. Jeder extern nachgeladene UEFI Code kann nur ausgeführt werden, wenn die Signaturprüfung erfolgreich ist. Auf dem Konnektor kommt ein Customized BIOS zum Einsatz, das ausschließlich den Public Key des Konnektor-Herstellers enthält. Somit kann vom BIOS aus nur Code ausgeführt werden, der mit dem geheimen Schlüssel des Herstellers signiert wurde. Das UEFI verifiziert die Signatur des Bootloaders und führt diesen aus. Im nächsten

Schritt wird die Signatur des Kernels vom Bootloader vor dessen Ausführung verifiziert. Der Kernel prüft die Signatur des Host-OS Images. Das Host-OS-Filesystem wird nur dann eingebunden, wenn die Signatur erfolgreich verifiziert werden konnte. Nach Einbinden des Host-OS-Images werden die Signaturen der einzelnen Images der virtuellen Maschinen auf korrektheit geprüft.

Mit diesem Prozess 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 oder über das Management-Interface anstoßen.

Schlägt die Prüfung der Integrität fehl, so wird der start up Prozess abgebrochen. Nach einem Neustart wird der Prozess erneut durchlaufen.

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).

Der private Authentisierungsschlüssel für das VPN wird bereits durch die 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 [92], Abschnitt 4.1.10 wie unter Sicherheitsdienst *Protokollierung* in Abschnitt 1.3.5.1 beschrieben. Diese Funktionalität ist mit FAU_GEN.1/NK.SecLog und FAU_GEN.2/NK.SecLog modelliert.

7.1.6. Administration

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

Der EVG verwaltet eine Administrator-Rolle (FMT_SMR.1./NK). Der Administrator muss autorisiert sein (FIA_UID.1/NK.SMR, FMT_SMR.1./NK und FMT_MSA.4/NK), bevor er administrative Tätigkeiten bzw. Wartungstätigkeiten ausführen darf (FMT_MTD.1/NK). Die Authentisierung erfolgt dabei durch den Netzkonnektor selbst.

Erst nach erfolgreicher Authentisierung wird ein entsprechender Autorisierungsstatus im EVG gesetzt (FMT_MSA.4/NK).

Die Wartung selbst erfolgt unter der Annahme, dass der Administrator über die LAN-Schnittstelle zugreift. Die Managementschnittstelle ist als REST-Schnittstelle implementiert. Der vorliegende EVG unterstützt keine Administratorrolle (Remote Administration), die aus dem Transportnetz zugreift.

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

Der Upate-Dienst des EVG kann über einen sicheren Kanal beim zentralen Konfigurationsdienst der TI (FTP_ITC.1/NK.KSR) Informationen über verfügbare Update-Pakete erhalten und automatisch oder manuell (durch den Administrator) in den vorgesehenen Speicherbereich laden. Alternativ kann auch über die lokale Managementschnittstelle ein Update-Paket bezogen werden (FTP_TRP.1/NK.Admin). Der Administrator wird informiert, wenn ein neues Update-Paket auf dem RISE-Konnektor vorliegt. Der Administrator kann daraufhin nach erfolgreicher Signaturprüfung des Update-Paketes die Integrität ((FDP_UIT.1/NK.Update) und Version prüfen und den Updateprozess anstoßen (FDP_ACC.1/NK.Update). Der EVG stellt sicher, dass Software Updates durch den lokalen Administrator freigeschaltet werden (FDP_ACF.1/NK.Update). Die Updates der Software des Konnektors können auch automatisch installiert werden, wenn dies explizit vom Administrator so konfiguriert wurde (FMT_MTD.1/NK).

Im Falle einer Software-Aktualisierung wird das aktuelle integere Software Image im EVG als „Fallback-Image“ beibehalten. Nach erfolgreicher Signaturprüfung des Update-Paketes wird das neue Software Image installiert. Erst wenn die Installation efolgreich abgelaufen ist, wird das neue Image aktiviert und ein Neustart durchgeführt. Schlägt die Signaturprüfung fehl oder kommt es während der Bootvorgangs zu Fehlern, wird das Update-Paket verworfen und das Fallback-Image wiederhergestellt. Nach erfolgreichem Neustart wird das Fallback-Image verworfen. Durch diesen Prozess wird verhindert, dass manipulierte Update-Pakete eingespielt werden können.

7.1.7. Kryptographische Basisdienste

Der Konnektor implementiert gemäß der Vorgaben des Dokuments „Übergreifende Spezifikation. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“ [*86*] die im Folgenden aufgelistete kryptographischen Primitive:

Der Konnektor Unterstützt Hash-Berechnung (FCS_COP.1/NK.Hash) und HMAC-Berechnung (FCS_COP.1/NK.HMAC) im Rahmen des Aufbaus von VPN Verbindungen. Die Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256 und RSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen (siehe FCS_COP.1/NK.Auth) wird vom Netzkonnektor mit Hilfe der *gSMC-K* durchgeführt.

Die Absicherung des IPsec-Tunnels erfolgt durch Ver- und Entschlüsselung mittels symmetrischer Algorithmen (AES im CBC Modus mit 256 Bit Schlüssellänge), siehe FCS_COP.1/NK.ESP. VPN Kommunikation erfolgt dabei nach dem IPsec Protocol (FCS_COP.1/NK.IPsec)

Die Schlüssel für die VPN-Kanäle werden mit hoher Qualität erzeugt (FCS_CKM.1/NK). Die Schlüsselerzeugung erfolgt 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). Der Schlüsselaustausch zum Aufbau von VPN-Tunnel erlogt nach IPsec IKEv2, siehe FCS_CKM.2/NK.IKE. Nicht mehr benötigte Schlüssel werden sofort vernichtet, siehe FCS_CKM.4/NK. Diese werden aktiv mit Nullen überschrieben.

Die kryptographischen Basisdienste (z.B. Hash-Berechnung, AES Ver-/Entschlüsselung) des Netzkonnektors werden nicht direkt nach außen zur Verfügung gestellt, sondern können nur indirekt aufgerufen werden (z.B. Einrichtung und Verwendung des VPN Kanals).

7.1.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Der Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung (FTP_ITC.1/NK.TLS). Dabei wird die TLS Funktionalität dem Anwendungskonnektor zur Verfügung gestellt der auch das Management der TLS Verbindung übernimmt (FMT_MOF.1/NK.TLS). Zertifikate die während des Aufbaus einer TLS-Verbindung zur Authentisierung verwendet werden, werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.

Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der Netzkonnektor das Exportieren von X.509 Zertifikate für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Managementschnittstelle (FDP_ETC.2/NK.TLS). Der Netzkonnektor bietet dabei die Möglichkeit solche Zertifikate und entsprechende RSA Schlüsselpaare zu erzeugen (FCS_CKM.1/NK.Zert). Die RSA Schlüssel werden nach dem Export durch das überschreiben mit festen Werten im EVG gelöscht (FCS_CKM.4/NK)

Die Zertifikate für die Anbindung der Clientsysteme können auch vom EVG gemäß FDP_ITC.2/NK.TLS über die gesicherte Managementschnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Diese werden beim Import nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert.

Für die TLS-Kanäle werden die sicheren kryptographische Algorithmen und Protokolle gemäß [76] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [*86*] implementiert.

Der Konnektor unterstützt HMAC-Berechnung (FCS_COP.1/NK.TLS.HMAC) im Rahmen des Aufbaus von TLS Verbindungen. Die Prüfung und Erzeugung von digitalen Signaturen (basierend auf SHA-256 und RSA/ECDSA Algorithmus) zur Unterstützung von Authentisierungsmechanismen (siehe FCS_COP.1/NK.TLS.Auth) wird vom Netzkonnektor mit Hilfe der *gSMC-K oder SMC-B* durchgeführt. Der EVG unterstützt ausschließlich sha256withRSAEncryption oder ecdsa-with-SHA256.

Nach erfolgreichem Verbindungsaufbau wird die Kommunikation mit AES gemäß FCS_COP.1/NK.TLS.AES abgesichert. Die Schlüssel für die TLS-Kanäle werden mit hoher Qualität erzeugt (FCS_CKM.1/NK.TLS). Nicht mehr benötigte Schlüssel werden sofort vernichtet, siehe FCS_CKM.4/NK. Diese werden aktiv mit Nullen überschrieben.

7.2. Abbildung der Sicherheitsfunktionalitäten des Netzkonnektors auf Sicherheitsanforderungen des Netzkonnektors

Tabelle 30 im folgenden Abschnitt 7.2.1 stellt die Abbildung der Sicherheitsfunktionalität auf Sicherheitsanforderungen zunächst tabellarisch im Überblick dar. In Abschnitt 7.2.2 wird die Abbildung erläutert und die Umsetzung der Anforderungen durch die Sicherheitsfunktionalität begründet.

7.2.1. Überblick

Sicherheitsanforderung an den EVG	7.1.1 VPN-Client	7.1.2 Dynamischer Paketfilter	7.1.3 Netzdienste	7.1.4 Stateful Packet Inspection	7.1.5 Selbstschutz	7.1.6 Administration	7.1.7 Kryptographische Basisdienste	7.1.8 TLS-Kanäle unter Nutzung sicherer
FTP_ITC.1/NK.VPN_TI	X							
FTP_ITC.1/NK.VPN_SIS	X							
FDP_IFC.1/NK.PF		X				X		
FDP_IFF.1/NK.PF		X		X				
FMT_MSA.3/NK.PF		X						
FMT_MSA.1/NK.PF		X				X		
FPT_STM.1/NK			X					
FPT_TDC.1/NK.Zert			X			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		
FTP_TRP.1/NK.Admin						X		X
FMT_SMF.1/NK						X		
FMT_MSA.4/NK						X		
FCS_COP.1/NK.Hash							X	
FCS_COP.1/NK.HMAC							X	
FCS_COP.1/NK.Auth							X	
FCS_COP.1/NK.ESP							X	
FCS_COP.1/NK.IPsec							X	
FCS_CKM.1/NK							X	
FCS_CKM.2/NK.IKE							X	
FCS_CKM.4/NK							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_ETC.2/NK.TLS								X

Sicherheitsanforderung an den EVG	7.1.1 VPN-Client	7.1.2 Dynamischer Paketfilter	7.1.3 Netzdienste	7.1.4 Stateful Packet Inspection	7.1.5 Selbstschutz	7.1.6 Administration	7.1.7 Kryptographische Basisdienste	7.1.8 TLS-Kanäle unter Nutzung sicherer
FDP_ITC.2/NK.TLS								X
FDP_ETC.2/AK.Enc								X
FMT_MOF.1/NK.TLS								X
FDP_ACC.1/NK.Update						X		
FDP_ACF.1/NK.Update						X		
FDP_UIT.1/NK.Update						X		
FTP_ITC.1/NK.KSR						X		

Tabelle 30: Abbildung der Sicherheitsfunktionalität des Netzkonnektors auf Sicherheitsanforderungen des Netzkonnektors

7.2.2. Erfüllung der funktionalen Sicherheitsanforderungen des Netzkonnektors

Wie aus der Tabelle 30 ersichtlich, wird jede Sicherheitsanforderung aus Kapitel 6.2 durch die Sicherheitsfunktionen in Kapitel 7.1 umgesetzt. Die Beschreibung der Sicherheitsfunktionen in den Kapiteln 7.1.1-7.1.8 nutzen direkte Referenzen auf die entsprechenden implementierten Sicherheitsfunktionen in den Kapiteln 6.2.1 bis 6.2.8. Die Sicherheitsfunktionen sind dabei direkt aus der Unterteilung der Sicherheitsfunktionen im PP BSI-CC-PP-0097-V2 [77] abgeleitet.

7.3. Anwendungskonnektor

Die zusammenfassende Spezifizierung des EVG wird in diesem Abschnitt und seinen Unterabschnitten anhand von funktionalen Gruppen gegliedert. Diese funktionalen Gruppen in den folgenden Abschnitten 7.3.1 bis 7.3.12 orientieren sich an den in Abschnitt 6.3 beschriebenen Sicherheitsanforderungen.

7.3.1. AK.Identifikation und Authentisierung

Der EVG implementiert unterschiedliche Mechanismen zur Identifikation und Authentisiserung von Benutzern (FIA_UAU.5/AK). Sicherheitsfunktionalität, die vor der Identifikation bzw. Authentisiserung von Subjekten verfügbar ist, ist in FIA_UAU.1/AK und FIA_UID.1/AK definiert.

Die Managementschnittstelle erfordert eine Passworteingabe, die vor unberechtigtem Zugriff schützt (FIA_SOS.1/AK.Passwörter). Die Kriterien an gültige Passwörter, die in FIA_SOS.1/AK.Passwörter aufgelistet sind, entstammen [92], TIP1-A_4808, werden vom Konnektor an die Benutzerpasswörter gestellt:

Für die Passwortverarbeitung setzt der Konnektor folgende Anforderungen um:

- Für die Erstanmeldung neuer Benutzer und beim Zurücksetzen von Benutzerpasswörtern durch den Super-Administrator werden Einmalpasswörter

generiert. Hierbei handelt es sich um Passwörter, die nach einmaligem Gebrauch bei der erstmaligen Anmeldung durch den Benutzer gewechselt werden müssen.

- Jeder Benutzer kann nach erfolgreicher Authentifizierung sein eigenes Passwort jederzeit ändern.
- Der Super-Administrator ist dafür verantwortlich, dass jeder Benutzer einen eigenen Benutzer-Account mit dazugehörigem Passwort verwendet und es keine gemeinsamen Benutzer gibt.
- Bei der Eingabe wird das Passwort nicht im Klartext auf dem Bildschirm angezeigt.
- Der RISE Konnektor initiiert nach einem durch den Super-Administrator konfigurierbaren Zeitraum einen Passwortwechsel beim nächsten Login.
- Erfolglose Anmeldeversuche werden mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt.
- Nach einer Fehleingabe des Passworts erfolgt eine drei Sekunden lange Verzögerung bis zur nächsten Eingabemöglichkeit des Passworts für dieselbe Benutzerkennung.

Im Rahmen des Pairing eines Kartenterminals generiert der Konnektor das „pairing secret“ mit hinreichend großer Entropie (FIA_SOS.2/AK.PairG). Wird ein angeschlossenes Kartenterminal für Stapel- oder Komfortsignaturen 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).

7.3.2. AK.Zugriffsberechtigungsdienst

Der Zugriffsberechtigungsdienst ist ein interner Dienst des Konnektors, der automatisch bei Aufruf einer Operation des Konnektors durch das Clientsystem ausgeführt wird. Durch den Zugriffsberechtigungsdienst 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.

7.3.3. AK.Kartenterminaldienst

Der Kartenterminaldienst des Konnektors verwaltet alle adressierbaren Kartenterminals. Dabei kapselt werden die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule gekapselt (FDP_ACC.1/AK.eHKT, FDP_ACF.1/AK.eHKT). Über den Kartenterminaldienst können TLS-Kanäle zu den Kartenterminals auf- und abgebaut werden sowie SICCT-Kommandos gesendet und empfangen werden.

Der Konnektor kommuniziert mit den angebundenen Kartenterminals über TLS-Kanäle (FDP_UCT.1/AK.TLS, FDP_UIT.1/AK.TLS). Der Netzkonnektor stellt diese Kommunikationskanäle für den Anwendungskonnektor zur Verfügung, vgl. Abschnitt 7.1.8.

Informationen über die Arbeitsplatzkonfiguration eines angeschlossenen Kartenterminals können vom Kartenterminaldienst ausgegeben werden (FMT_MTD.1/AK.eHKT_Abf).

Ausschließlich der Administrator darf diese Konfiguration verändern (FMT_MTD.1/AK.eHKT_Mod).

7.3.4. AK.Chipkartendienst

Die Kartenterminals, die am Konnektor angebunden sind, können verschiedene Chipkartentypen (KVK, eGK, SMC-B und HBA) aufnehmen. Die in den Kartenterminals eines Arbeitsplatzes gesteckten Chipkarten mit ihren logischen Kanälen bilden einen dynamischen Kontext (siehe [92]). Die Identifikation dieser Chipkarten erfolgt durch Kartenhandles. Der EVG stellt Sicherheitsfunktionen des Chipkartendienstes anderen Diensten, dem Clientsystem oder den Fachmodulen bereit (FDP_ACC.1/AK.KD). Dazu gehören der Aufbau und die Verwaltung logischer Kanäle und die Kommunikation mit den Karten unter Verwendung spezieller 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 entfernte PIN-Eingabe an den Kartenterminals umgesetzt (FDP_ACC.1/AK.PIN) und die unterschiedlichen Anforderungen an lokale und entfernte 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).

7.3.5. AK.Signaturdienst

Der EVG unterstützt in diesem Anteil der TSF verschiedene Signaturtypen und -varianten. Diese Typen und Varianten erlauben es, sogenannte Signaturrichtlinien im Aufruf der Schnittstelle anzugeben, die dafür sorgen, dass entsprechend erzeugte Dokumentensignaturen einem vorgegebenen Schema folgen. Verursacht durch die gleichzeitige Relevanz der Konnektor-Spezifikation [92] und des BSI-CC-PP-0098-V3 unterliegt der Begriff „Signaturrichtlinie“ im Rahmen dieser Sicherheitsvorgaben einer kontextabhängigen Semantik:

(a) Signaturrichtlinie als Funktionsparameter für genau diejenige Dokumentensignatur, welche durch die Funktion ausgelöst wird. Diese Festlegung entspringt der Heuristik von [92].
(b) Signaturrichtlinie in der Bedeutung einer funktionalen Beschreibung (insbesondere der Einschränkungen) der Konnektorschnittstelle zur Signaturerzeugung und -prüfung.

Beispielsweise handelt es sich bei der NFDM-Signaturrichtlinie [110] um die Semantik (a). In Abgrenzung hierzu beschreibt das Herstellerdokument [RISE-KON-SRLRQ] die Signaturschnittstelle des EVG auf funktionaler Ebene.

Der Signaturdienst bietet Clientsystemen und Fachmodulen die Möglichkeit, Dokumente zu signieren (FDP_ACC.1/AK.Sgen, FDP_ACF.1/AK.Sgen) und Dokumentensignaturen zu prüfen (FDP_ACC.1/AK.SigPr, FDP_ACF.1/AK.SigPr). Die zu signierenden bzw. zu prüfenden Daten werden vom Konnektor entsprechend der referenzierten Signaturrichtlinie behandelt. Die angegebene Signaturrichtlinie wird beim Import auf Zulässigkeit geprüft (FDP_ITC.2/AK.Sig, FMT_MSA.3/AK.Sig). Die Plattform des Konnektors stellt selbst keine

Signaturrichtlinien bereit. Das vom EVG 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). Außerdem 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 verwaltetet. 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 Integritätsprüfung der erhaltenen Signatur vom EVG festgestellt werden (FDP_SDI.2/AK).

Der Signaturdienst unterstützt das folgende Signaturformat für QES:

- XAdES für XML Dokumente, nach NFDM-Richtlinie [110].

Außerdem unterstützt der EVG die folgenden Signaturformate für QES und nonQES:

- CAdES für XML, PDF/A, Text und TIFF Dokumente
- PAdES für PDF/A Dokumente.

Darüber hinaus werden für nonQES die folgenden Signaturformate unterstützt

- CAdES für Binärdateien
- S/MIME für Multipurpose Internet Mail Extensions,

Die zur Signaturerstellung verwendeten kryptographischen Algorithmen sind RSASSA-PSS mit SHA-256 (nach FCS_COP.1/AK.XML.Sign, FCS_COP.1/AK.CMS.Sign und 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 (FCS_COP.1/AK.SHA)

Die Signaturberechnung erfolgt durch die Signaturkarte mit RSASSA-PSS.

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 angegebene 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 zeigt 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 an. Diese Jobnummer wird vom Konnektor im Display des eHealth-Kartenterminals neben der PIN-Eingabeaufforderung angezeigt (FTA_TAB.1/AK.Jobnummer).

Das Prüfen von Dokumentensignaturen erfolgt auf Basis von Zertifikaten (FDP_DAU.2/AK.Cert). Die Feststellung einer ungültig erzeugten Signatur wird dem Benutzer durch eine Warnmeldung angezeigt (FTA_TAB.1/AK.SP).

Für die Signaturprüfung werden zudem für nonQES und QES die Signaturformate PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v1_**5** unterstützt.

Die folgende Tabelle gibt eine Übersicht über alle für die Signaturprüfung umgesetzten Kombinationen von Formaten, Signaturverfahren und Hashalgorithmen für QES und nonQES. Dies entspricht den Festlegungen in

- FCS_COP.1/AK.SigVer.ECDSA,
- FCS_COP.1/AK.SigVer.PSS,
- FCS_COP.1/AK.SigVer.SSA,
- FCS_COP.1/AK.XML.SigPr,
- FCS_COP.1/AK.CMS.SigPr,
- FCS_COP.1/AK.PDF.SigPr,

Geheime kryptographische Schlüssel, zu signierende Daten und signierte Daten werden nach Verwendung durch den Konnektor unzugänglich gemacht (FDP_RIP.1/AK).

Signaturtyp[323]	QES / non QES	Signaturverfahren	Schlüssellänge	Hashalgorithmen
XMLDSig (XAdES) FCS_COP.1/AK.XML.SigPr	**QES**	RSASSA-PKCS1-v1_5 (FCS_COP.1/AK.SigVer. SSA in Verbindung mit FCS_COP.1/AK.SHA)	**1976 – 4096 bit**	**SHA-256** **SHA-384** **SHA-512**
		RSASSA-PSS (FCS_COP.1/AK.SigVer. PSS in Verbindung mit FCS_COP.1/AK.SHA)	**1976 – 4096 bit**	**SHA-256** **SHA-384** **SHA-512**
		ECDSA (FCS_COP.1/AK.SigVer. ECDSA)	**256bit**	**SHA-256**
PDF/A (PAdES) FCS_COP.1/AK.PDF.SigPr **CMS (CAdES)** FCS_COP.1/AK.CMS.SigPr	**QES**	RSASSA-PKCS1-v1_5 (FCS_COP.1/AK.SigVer. SSA in Verbindung mit FCS_COP.1/AK.SHA)	**1976 – 4096 bit**	**SHA-256** **SHA-384** **SHA-512**
		RSASSA-PSS (FCS_COP.1/AK.SigVer. PSS in Verbindung mit FCS_COP.1/AK.SHA)	**1976 – 4096 bit**	**SHA-256** **SHA-384** **SHA-512**
		ECDSA (FCS_COP.1/AK.SigVer. ECDSA)	**256bit**	**SHA-256**
	nonQES	RSASSA-PSS (FCS_COP.1/AK.SigVer. PSS in Verbindung mit FCS_COP.1/AK.SHA)	**2048 bit**	**SHA-256**
		ECDSA (FCS_COP.1/AK.SigVer. ECDSA)	**2048 bit**	**SHA-256**
S/MIME FCS_COP.1/AK.CMS.SigPr	**nonQES**	RSASSA-PSS (FCS_COP.1/AK.SigVer. PSS in Verbindung mit FCS_COP.1/AK.SHA)	**2048 bit**	**SHA-256**
		ECDSA (FCS_COP.1/AK.SigVer. ECDSA)	**2048 bit**	**SHA-256**

Tabelle 31: Übersicht der Kombinationen von Formaten, Signaturverfahren und Hashalgorithmen für die Signaturprüfung

Der EVG unterstützt neben der Einzel- und Stapelsignatur auch die Funktion der Erstellung einer Komfortsignatur über einen vertrauenswürdigen Kanal (Secure Messaging, FTP_ITC.1/AK.QSEE, FIA_API.1/AK). Dabei stellt das Praxisverwaltungssystem des

[323] Gemäß `dss:SignatureObject` in [**Fehler! Textmarke nicht definiert.**], TAB_KON_066.

Leistungserbringers sicher, dass nur berechtigte Benutzer die Komfortsignatur am Praxisverwaltungssystem auslösen können. Durch den EVG wird sichergestellt (FDP_ACC.1/AK.Sgen, FDP_ACF.1/AK.Sgen), dass eine Komfortsignatur nur nach vorheriger globaler Aktivierung der Funktion durch den Administrator, nach Aktivierung der Funktion durch den Benutzer und nach dem Setzen der maximalen Anzahl von per Komfortsignatur erzeugbaren Signaturen durch den Benutzer möglich ist. Weiterhin werden bei der Erstellung einer Komfortsignatur der Aufrufkontext und die Eigenschaften der UserID (Format und Länge) durch den EVG überprüft (FIA_UAU.5/AK). Entsprechend wird bei der Komfortsignatur der Authentisierungsstatus der PIN nicht nach jeder Signatur zurückgesetzt, sondern wenn a) die Funktion Komfortsignatur deaktiviert wird, b) der Zähler SAK_COMFORT_SIGNATURE_TIMER den eingestellten Maximalwert erreicht hat oder c) die maximal Anzahl an erlaubten Signaturen (Zähler SAK_COMFORT_SIGNATURE_MAX) erreicht wurde (FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK). Der EVG informiert Clientsysteme gemäß FTA_TAB.1/AK.SP über Abweichungen beim Signaturprozess.

7.3.6. AK.Verschlüsselungsdienst

Analog zu den Ausführungen in Abschnitt 7.3.5 unterliegt der Begriff „Verschlüsselungsrichtlinie“ im Rahmen dieser Sicherheitsvorgaben einer kontextabhängigen Semantik:

(a) Verschlüsselungsrichtlinie als Funktionsparameter für genau diejenige Dokumentenverschlüsselung, welche durch die Funktion ausgelöst wird. Diese Festlegung entspringt der Heuristik von [92].

(c) Verschlüsselungsrichtlinie in der Bedeutung einer funktionalen Beschreibung (insbesondere der Einschränkungen) der Konnektorschnittstelle zur Verschlüsselung.

Die Spezifikation [92] sieht keine Verschlüsselungsrichtlinie nach (a) vor und entsprechend können solche nicht als Paramater an der Schnittstelle zum Konnektor verwendet werden. Die funktionale Beschreibung findet sich in [RISE-KON-FSP], Abschnitt 17.2.24 f.

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 RFC 5652 [34] bzw. die symmetrische Ver-/Entschlüsselung mittels AES-GCM an. Zudem wird für XML-Dokumente die hybride Ver-/Entschlüsselung nach XML Encryption Syntax and Processing [21] unterstützt und für MIME-Dokumenten die hybride Ver-/Entschlüsselung nach RFC 5751 [35] unterstützt.

Das Clientsystem übergibt die zu verschlüsselnden bzw. zu entschlüsselnden Dokumente. Die zu verwendende Verschlüsselungsrichtlinie wird 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 und AES-GCM mit 256 Bit Schlüssellänge und 128 Bit GMAC (FCS_COP.1/AK.XML.Ver, FCS_COP.1/AK.XML.Ent)
- MIME-Dokumente: RSAOAEP mit 2048 Bit Schlüssellänge und AES-GCM mit 256 Bit Schlüssellänge und 128 Bit (FCS_COP.1/AK.MIME.Ver, FCS_COP.1/AK.MIME.Ent)
- XML, PDF/A, Text, TIFF und Binärdaten: RSAOAEP mit 2048 Bit Schlüssellänge und AES-GCM mit 256 Bit Schlüssellänge und 128 Bit (FCS_COP.1/AK.CMS.Ver, FCS_COP.1/AK.CMS.Ent)

Der EVG erzeugt die AES Schlüssel (FCS_CKM.1/AK.AES) und löscht diese nach Verwendung sicher (FCS_CKM.4/AK).

Der Konnektor macht geheime Kryptographische Schlüssel, zu verschlüsselnde Daten, verschlüsselte Daten, vorgeschlagene Empfänger und entschlüsselte Daten nach Verwendung unzugänglich (FDP_RIP.1/AK).

7.3.7. AK.TLS-Kanäle

Der Netzkonnektor stellt dem Anwendungskonnektor TLS-Kanäle zur Verfügung, siehe Abschnitt 7.1.8. Die Verwaltung von TLS-Kanälen wird duch den Anwendungskonnektor durchgeführt.

Der Anwendungskonnektor initiiert dabei entsprechend der Vorgaben in Tabelle 23 den Auf- und Abbau der TLS-Känale und stellt den Endpunkt für das Senden und Empfangen der Nutzdaten dar (FDP_ACC.1/AK.TLS, FDP_ACF.1/AK.TLS). Für das Fachmodul VSDM 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 bzw. äquivalent FTP_ITC.1/NK.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).

7.3.8. AK.Sicherer Datenspeicher

Der EVG besitzt einen sicheren Datenspeicher, in dem alle sicherheitsrelevanten, veränderlichen Daten dauerhaft speichert werden (FDP_ACC.1/AK.SDS,

FDP_ACF.1/AK.SDS). Dieser Datenspeicher sichert die Integrität, Authentizität und Vertraulichkeit der Daten, die dort hinterlegt bzw. abgerufen werden. Der Konnektor stellt den vorhandenen Fachmodulen ebenfalls die Nutzung eines sicheren Datenspeichers für ihre sensiblen Daten zur Verfügung.

Im EVG werden keine Datenobjekte mit dem Sicherheitsattribut „Administratorobjekt“ verwaltet.

7.3.9. AK.Fachmodul VSDM

Das Fachmodul VSDM ist fester Bestandteil des EVG 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.Chipkartendienst angesprochen. Das Fachmodul VSDM kann über die Management-Oberfläche administriert werden (FMT_MSA.1/AK.VSDM, FMT_MSA.3/AK.VSDM).

7.3.10. AK.Sicherheitsmanagement

Der Konnektor verwaltet verschiedene Rollen, wie Adminstrator, Clientsystem, Kartenterminals und Chipkarten (FMT_SMR.1/AK). Auf die Managementschnittstelle hat nur ein autorisierter Administrator Zugriff. Dieser kann zum Beispiel Kartenterminals managen, Arbeitsplätze Konfigurieren, Sicherheitsrichlinien und TLS-Kanäle verwalten (FMT_SMF.1/AK). Dazu gehört auch das Verwalten von Software-Updates für den EVG und angebundene Kartenterminals, Verwalten von Zertifikaten und Durchführen eines Werksresets (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 aktivieren und deaktivieren (MGM_LU_SAK**)**, (FMT_MOF.1/AK). 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).

7.3.11. AK.Schutz der TSF

Der Konnektor kann die für QES und nonQES benötigten Zertifikate interpretieren. 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 von Daten, die importiert zu signierenden bzw. zu prüfen sind, wird gemäß implementierter Signaturrichtlinien geprüft. Durch das Fachmodul NFDM wird eine entsprechende Signaturrichtlinie in den Konnektor eingebracht.

Der Konnektor setzt die in [92], TAB_KON_503, definierten Fehlbetriebszustände um (Error Condition). Wird ein sicherheitsrelevanter Betriebszustand erreicht, schränkt der Konnekotr seine Funktionalität gemäß [92], TAB_KON_504, ein (FPT_FLS.1/AK).

Vor der regulären Kommunikation mit einem 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, FPT_TST.1/AK.Out-Of-Band), siehe dazu auch Abschnitt 7.1.5.

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 Abschnitt 7.1.3.

7.3.12. AK.Sicherheitsprotokollierung

Der EVG führt ein Sicherheits-Log gemäß Konnektor-Spezifikation [92], Abschnitt 4.1.10, siehe auch „Sicherheits-Log“ in 7.1.5. 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).

7.3.13. VAU-Kommunikation

Der Konnektor stellt dem Fachmodul ePA einen Kommunikationskanal (VAU-Kommunikation) zur Kommunikation mit der VAU des ePA-Aktensystems zur Verfügung (FTP_ITC.1/VAU). Dieser stellt gemäß [*86*] den Endpunkt für das Senden und Empfangen der Nutzdaten dar.

Die Verwaltung der VAU-Kommunikation, die gemäß FPT_TDC.1/VAU auf Authentizität und Integrität geprüft wird, wird durch das Fachmodul ePA durchgeführt. Das im Rahmen der VAU-Kommuniktion generierte ephemere Schlüsselmaterial (FCS_CKM.1/VAU) wird nach Ende der Nutzung in der VAU-Kommunikation (FCS_COP.1/VAU) sicher zerstört (FCS_CKM.4/AK).

7.3.14. SGD-Kommunikation

Der Konnektor stellt dem Fachmodul ePA einen Kommunikationskanal (SGD-Kommunikation) zur Kommunikation mit dem HSM des Schlüsselgenerierungsdienstes zur Verfügung (FTP_ITC.1/SGD). Dieser stellt gemäß [87] den Endpunkt für das Senden und Empfangen der Nutzdaten dar. Der EVG prüft die Identität des SGD-HSM gemäß FPT_TDC.1/SGD.Zert. Das vom SGD-HSM übermittelte Schlüsselmaterial wird gemäß FDP_ITC.1/SGD importiert.

Die Verwaltung der SGD-Kommunikation wird nach den Zugriffsregeln in FDP_ACC.1/SGD und FDP_ACF.1/SGD durch das Fachmodul ePA durchgeführt. Das im Rahmen der VAU-Kommuniktion generierte ephemere Schlüsselmaterial (FCS_CKM.1/SGD) wird nach Ende der Nutzung in der SGD-Kommunikation (FCS_COP.1/SGD) sicher zerstört (FCS_CKM.4/AK).

7.4. Abbildung der Sicherheitsfunktionalitäten des Anwendungskonnektors auf Sicherheitsanforderungen des Anwendungskonnektors

7.4.1. Überblick

	7.3.1 AK.Identifikation und Authentisierung	7.3.2 AK.Zugriffsberechtigungsdienst	7.3.3 AK.Kartenterminaldienst	7.3.4 AK.Chipkartendienst	7.3.5 AK.Signaturdienst	7.3.6 AK.Verschlüsselungsdienst	7.3.7 AK.TLS-Kanäle	7.3.8 AK.Sicherer Datenspeicher	7.3.9 AK.Fachmodul VSDM	7.3.10 AK.Sicherheitsmanagement	7.3.11 AK.Schutz der TSF	7.3.12 AK.Sicherheitsprotokollierung	7.3.13. VAU-Kommunikation	7.3.14. SGD-Kommunikation
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							X	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									
FCS_COP.1/AK.MIME.Ent						X								
FCS_COP.1/AK.MIME.Ver						X								
FCS_COP.1/AK.XML.Ent						X								
FCS_COP.1/AK.XML.Sign					X									

	7.3.1 AK.Identifikation und Authentisierung	7.3.2 AK.Zugriffsberechtigungsdienst	7.3.3 AK.Kartenterminaldienst	7.3.4 AK.Chipkartendienst	7.3.5 AK.Signaturdienst	7.3.6 AK.Verschlüsselungsdienst	7.3.7 AK.TLS-Kanäle	7.3.8 AK.Sicherer Datenspeicher	7.3.9 AK.Fachmodul VSDM	7.3.10 AK.Sicherheitsmanagement	7.3.11 AK.Schutz der TSF	7.3.12 AK.Sicherheitsprotokollierung	7.3.13. VAU-Kommunikation	7.3.14. SGD-Kommunikation
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.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.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							

	7.3.1 AK.Identifikation und Authentisierung	7.3.2 AK.Zugriffsberechtigungsdienst	7.3.3 AK.Kartenterminaldienst	7.3.4 AK.Chipkartendienst	7.3.5 AK.Signaturdienst	7.3.6 AK.Verschlüsselungsdienst	7.3.7 AK.TLS-Kanäle	7.3.8 AK.Sicherer Datenspeicher	7.3.9 AK.Fachmodul VSDM	7.3.10 AK.Sicherheitsmanagement	7.3.11 AK.Schutz der TSF	7.3.12 AK.Sicherheitsprotokollierung	7.3.13. VAU-Kommunikation	7.3.14. SGD-Kommunikation
FDP_SDI.2/AK					X									
FDP_UCT.1/AK.TLS			X											
FDP_UIT.1/AK.TLS			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			

	7.3.1 AK.Identifikation und Authentisierung	7.3.2 AK.Zugriffsberechtigungsdienst	7.3.3 AK.Kartenterminaldienst	7.3.4 AK.Chipkartendienst	7.3.5 AK.Signaturdienst	7.3.6 AK.Verschlüsselungsdienst	7.3.7 AK.TLS-Kanäle	7.3.8 AK.Sicherer Datenspeicher	7.3.9 AK.Fachmodul VSDM	7.3.10 AK.Sicherheitsmanagement	7.3.11 AK.Schutz der TSF	7.3.12 AK.Sicherheitsprotokollierung	7.3.13. VAU-Kommunikation	7.3.14. SGD-Kommunikation
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							
FTP_ITC.1/AK.FD							X							
FTP_ITC.1/AK.QSEE					X									
FTP_ITC.1/AK.VZD							X							
FTP_ITC.1/AK.TSL							X							
FTP_ITC.1/AK.KSR							X							
FTP_ITC.1/VAU													X	
FPT_TDC.1/VAU													X	
FCS_CKM.1/VAU													X	
FCS_COP.1/VAU													X	
FPT_TDC.1/SGD.Zert														X
FTP_ITC.1/SGD														X
FCS_COP.1/SGD.AES														X
FCS_CKM.1/SGD.ECIES														X
FCS_COP.1/SGD.ECIES														X
FDP_ITC.1/SGD														X
FDP_ACC.1/SGD														X
FDP_ACF.1/SGD														X

Tabelle 32: Abbildung der Sicherheitsfunktionalität des Anwendungskonnektors auf Sicherheitsanforderungen des Anwendungskonnektors

7.4.2. Erfüllung der funktionalen Sicherheitsanforderungen des Anwendungskonnektors

Wie aus der Tabelle 32 ersichtlich, wird jede Sicherheitsanforderung aus Kapitel 6.3 durch die Sicherheitsfunktionen in Kapitel 7.3 umgesetzt. Die Beschreibung der Sicherheitsfunktionen in den Kapiteln 7.3.1-7.3.12 nutzen direkte Referenzen auf die entsprechenden implementierten Sicherheitsfunktionen in den Kapiteln 6.3.1 bis 6.3.6.

8. Erfassung von zusätzlichen Anforderungen

8.1. Anforderungen resultierend aus der Produkttypversion 3

Das Protection Profile BSI-CC-PP-0098-V3, das diesem Security Target zugrunde liegt, erfasst alle Sicherheitsanforderungen, die für Produkttypversion 2 (vgl. [88]) des Konnektors vorgesehen sind. Vorliegender EVG realisiert jedoch bereits Produkttypversion 3 (vgl. [89]) und höher und hat entsprechend [89] und [93] über das Protection Profile hinausgehende Sicherheitseigenschaften im Rahmen der CC-Evaluierung nachzuweisen. Die folgende Tabelle erfasst diese zusätzlichen Sicherheitseigenschaften für Produkttypversion 3 und gibt eine Erläuerung, wie diese im vorliegenden Security Target erfasst sind. [324]

Anforderung aus [89] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
TIP1-A_4710	Medizinische Daten oder personenbezogene Daten (darunter KVNR, ICCSN und CardHolderName) dürfen nicht in Protokolleinträge geschrieben werden.	In Anwendungshinweis 203 erfasst. *Bereits im PP so erledigt, 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 im PP so erledigt, 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.	Erfassung in Sicherheitsvorgaben obsolet; 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. Der Schutz der Konfigurationsdaten beim Austausch zwischen Clientsystem und EVG ist Gegenstand der Transportsicherung, vgl. Tabelle 35 (Transportsicherung).
TIP1-A_5486	Aktivieren/Deaktivieren des PIN-Schutzes	*Bereits im PP ab Version 1.4 so erledigt, keine besondere Anpassung in diesem Security Target.*
TIP1-A_5505	Kryptographische Prüfung der XML-Dokumentensignatur gemäß TUC_KON_162	*Siehe* Tabelle 34*, TUC_KON_162*
TIP1-A_5538	Signaturrichtlinien bei QES für XML-Dokumentenformate	In FPT_TDC.1.2/AK (9) wurde die Auswahl „Signaturrichtlinie“

[324] Für die Anforderungen gemäß Produkttypversion 4 siehe die Abschnitt 8.3 und 8.4

Anforderung aus [89] i.V.m. [93]	Inhaltlicher Abriss der Anforderung	Umsetzung im vorliegenden Security Target
		eingeschlossen. Außerdem: Anwendungshinweis 46 und Hinweis darunter.
TIP1-A_6025	Zugang zur TI sperren, wenn Deadline für kritische FW-Updates erreicht ist.	In Anwendungshinweis 198 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 35.
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	Siehe Anwendungshinweis 102 und FIA_UAU.5/AK. Der vorliegende EVG unterstützt kein Remote Management.
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	Siehe Anwendungshinweis 102. Der vorliegende EVG unterstützt kein Remote Management.
TIP1-A_7279	Authentifizierung des Remote-Administrators	Siehe FIA_UAU.5/AK. Remote Administrator Rollen werden vom EVG nicht umgesetzt.
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	Der vorliegende EVG unterstützt kein Remote Management.
GS-A_5484 (gemSpec_PKI)	Aktualisierung der BNetzA-VL	Entspricht TIP1-A_6729 von [88] und war schon in PTV2 der CC-Evaluierung zugerechnet. Umgesetzt in BSI-CC-PP-0098-V3.
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 33: Über BSI-CC-PP-0098-V3 hinausgehende Anforderungen an die CC-Evaluierung des Konnektors PTV3

8.2. Anforderungen resultierend aus der Unterstützung der Fachmodule AMTS und NFDM

Der RISE Konnektor V3.0 unterstützt die Fachmodule NFDM (nach [108]) und AMTS (nach [109]).

Entsprechend der Technischen Richtlinien TR-03154 [82] und TR-03155 [83], Kapitel 3.3.2, gelten Anforderungen an den Konnektor, die im Rahmen der Evaluierung betrachtet werden müssen. Diese werden im Folgenden zusammengefasst.

Der Anwendungskonnektor stellt den Fachmodulen NFDM und AMTS bestimmte Funktionen der Basisdienste zur Verfügung, die von den Fachmodulen über entsprechende Schnittstellen zum Konnektor aufgerufen werden können. In Tabelle 34 werden die nach TR-03154 und TR-03155 sicherheitsrelevanten Funktionen der Basisdienste anhand der in [93] definierten Technical Use Cases (TUC) aufgelistet und die jeweilige dem Fachmodul angebotene Schnittstelle angegeben.

Dienst	**TUC nach [93]**	**Konnektor-Schnittstelle zum Fachmodul**	**Fach-module**
Zugriffsberechtigungsdienst	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Siehe [RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Dokumentenvalidierungsdienst	TUC_KON_080 „Dokument validieren“ (indirekt)	[RISE-KON-SGFM], Abschnitt 4	NFDM
Kartendienst	TUC_KON_005 „Card-to-Card authentisieren“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_012 „PIN verifizieren“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_018 „eGK-Sperrung prüfen“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_022 „Liefere PIN-Status“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_026 „Liefere CardSession“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_036 „Liefere Fachliche Rolle“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_041 „Einbringen der Endpunktinformationen während der Bootup-Phase“	[RISE-KON-SGFM], Abschnitt 4	AMTS
Kartendienst	TUC_KON_202 „Lese Datei“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_203 „Schreibe Datei“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Kartendienst	TUC_KON_204 „Lösche Datei Inhalt“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS

Kartendienst	TUC_KON_221 „Liefere Anwendungsstatus“	Dieser TUC wird zwar von der TR AMTS, Abschnitt 3.3.2 gefordert, ist jedoch weder spezifiziert noch vom EVG umgesetzt oder vom FM AMTS verwendet.	AMTS
Kartenterminaldienst	TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Signaturdienst	TUC_KON_151 „QES Dokumentensignatur prüfen“	[RISE-KON-SGFM], Abschnitt 4	NFDM
Signaturdienst	TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“	[RISE-KON-SGFM], Abschnitt 4	NFDM
Systeminformationsdienst	TUC_KON_254 "Liefere Ressourcendetails"	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Protokollierungsdienst	TUC_KON_271 „Schreibe Protokolleintrag“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Zeitdienst	TUC_KON_351 „Liefere Systemzeit“	[RISE-KON-SGFM], Abschnitt 4	NFDM, AMTS
Zertifikatsdienst	TUC_KON_034 „Zertifikatsinformationen extrahieren“	[RISE-KON-SGFM], Abschnitt 4	NFDM

Tabelle 34: Sicherheitsrelevante Schnittstellen für die Fachmodule AMTS und NFDM

Die korrekte Nutzung der Schnittstellen durch die Fachmodule ist Gegenstand der TR-Zertifizierung nach den Technischen Richtlinien 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 6.4.5, Verfeinerungen hinsichtlich der Fachmodule NFDM,AMTS.

Darüber hinaus werden in den Technischen Richtlinien der Fachmodule weitere Sicherheitsanforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung betrachtet werden müssen. Diese werden in der folgenden Tabelle behandelt:

Anforderungen aus TR	**Umsetzung durch den Konnektor**
(Nur NFDM) Signaturdienst - QES-Prüfung von XML-detached Signaturen (nach vorheriger Prüfung gemäß gematik Signaturrichlinie 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

Anforderungen aus TR	Umsetzung durch den Konnektor
	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 duch die Sicherheitsfunktionen 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 Managementschnittstelle des Konnektors auslesen. Im Benutzerhandbuch findet sich die entsprechende Beschreibung.

Tabelle 35: Weitere Anforderungen an den Konnektor induziert durch die Technischen Richtlinien für die Fachmodule NFDM und AMTS

8.3. Anforderungen resultierend aus der Produkttypversion 4

Das Protection Profile BSI-CC-PP-0098-V3, das diesem Security Target zugrunde liegt, erfasst alle Sicherheitsanforderungen, die für Produkttypversion 2 (vgl. [88]) des Konnektors vorgesehen sind. Vorliegender EVG realisiert jedoch bereits Produkttypversion 4 (vgl. [90]) und höher und hat entsprechend [90] und [93] über das Protection Profile und die oben genannten Anfordeurngen aus Produkttypversion 3 hinausgehende Sicherheitseigenschaften im Rahmen der CC-Evaluierung nachzuweisen. Die folgende Tabelle erfasst diese zusätzlichen Sicherheitseigenschaften (zusätzlich zu Produkttypversion 3) und gibt eine Erläuerung, wie diese im vorliegenden Security Target erfasst sind.

Anforderung aus [90] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
A_16203	Im Zustand EC_Firewall_Not_Reliable DARF der Konnektor NICHT nutzbar sein.	Siehe Anwendungshinweis 198.
A_17225	Der Konnektor MUSS für Fachmodule den Aufbau einer sicheren Verbindung zur Vertrauenswürdigen Ausführungsumgebung (VAU) unterstützen	Siehe Abschnitt 6.3.7 und FTP_ITC.1/VAU
A_17548	TSL-Signer-CA Cross-Zertifikat sicher speichern	Ergänzung in Anwendungshinweis 89:
A_17549	Import TSL-Signer-CA Cross-Zertifikat im kritischen Zustand ermöglichen.	Ergänzung in Anwendungshinweis 198:
A_17661	Gesicherte Übertragung der Hash-Datei für TSL	Ergänzung in Anwendungshinweis 88: und FDP_ACF.1/AK.TLS
A_17746	Einsatzbereich und Vorgaben für Ver- und Entschlüsselung	Ergänzung der Anwendungshinweise Anwendungshinweis 143: und Anwendungshinweis 145: sowie Hinweis in FCS_COP.1/AK.MIME.Ver und FCS_COP.1/AK.CMS.Ver
A_17768	Zertifikate und Schlüssel für Signaturerstellung und Signaturprüfung	Ergänzung in Anwendungshinweisen Anwendungshinweis 127:, Anwendungshinweis 129:, Anwendungshinweis 132:, Anwendungshinweis 133:, Anwendungshinweis 134:, Anwendungshinweis 135:, Anwendungshinweis 136:, Anwendungshinweis 137:, Anwendungshinweis 138:, Anwendungshinweis 139:
A_17777	Der Konnektor MUSS für Fachmodule für die Nutzung der Schlüsselableitungsfunktionalität die sicherheitstechnischen Festlegungen gemäß [gemSpec_Krypt#3.15.5 Schlüsselableitungsfunktionalität ePA] und [gemSpec_SGD] bereitstellen.	Siehe Abschnitt 6.3.8 und FTP_ITC.1/SGD
A_17837−01	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA	Ergänzung in Anwendungshinweis 88:
A_18001	TUC_KON_075 „Symmetrisch verschlüsseln”	Ergänzung in Anwendungshinweis 141:
A_18002	TUC_KON_076 „Symmetrisch entschlüsseln”	Ergänzung in Anwendungshinweis 141:
TIP1−A_4510−02	Begrenzung im Fall von Fehlerzuständen (Tab_ Kon_503 Betriebszustand_Fehlerzustandsliste)	Anpassung in FPT_FLS.1/AK an neue Version der Konnektor Spezifikation
TIP1−A_4569−02	TUC_KON_021 „PIN entsperren“	Nur redaktionelle Änderungen der bereits in PTV2 vorhandenen und daher in BSI-CC-PP-0098-V3 modellierten Anforderung TIP1-A_4569.
TIP1−A_4646−02	TUC_KON_155 „Dokumente zur Signatur	Anforderung bringt inhaltliche Klarstellungen, ist grundsätzlich aber bereits in PTV2 enthalten => keine Änderung im ST PTV4
TIP1−A_4653−02	TUC_KON_160 „Dokumente nonQES	Anforderung bringt inhaltliche Klarstellungen, ist grundsätzlich aber

Anforderung aus [90] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
		bereits in PTV2 enthalten => keine Änderung im ST PTV4
TIP1−A_4654−02	„nonQES Dokumentsignatur prüfen"	Anforderung bringt inhaltliche Klarstellungen, ist grundsätzlich aber bereits in PTV2 enthalten => keine Änderung im ST PTV4
TIP1−A_4785−02	Konfigurationsparameter VPN-Client in Admin Schnittstelle	keine relevanten Änderungen in Afo
TIP1−A_4832−02	TUC_KON_280 „Konnektoraktualisierung	keine relevanten Änderungen in Afo
TIP1−A_4839−01	Festlegung der durchzuführenden Updates	keine relevanten Änderungen in Afo
TIP1−A_4840−01	Manuelles Auslösen der durchzuführenden Updates	keine relevanten Änderungen in Afo
TIP1−A_5541−01	Externe Ressourcen nicht auflösen	Anforderung bringt inhaltliche Klarstellungen, ist grundsätzlich aber bereits in PTV2 enthalten => keine Änderung im ST PTV4
TIP1−A_5657−02	Freischaltung von Softwareupdates	keine relevanten Änderungen in Afo
A_15549	VAU-Client: Kommunikation zwischen VAU-Client	FTP_ITC.1/VAU
A_15561	Bevorzugte Nutzung von AES-NI wenn vorhanden.	EVG verwendet AES-NI nicht.
A_16849	VAU-Protokoll: Wenn ein Client oder ein Server den Protokollablauf nach Protokollbeschreibung abbrechen muss, dann MUSS dieser die eventuell aktuell vorhandene KeyID aus seiner Datenbasis löschen und die damit verbundenen Schlüssel sicher löschen.	Mit FCS_CKM.4/AK abgedeckt.
A_16852	VAU-Protokoll: ECDH durchführen.	Siehe FCS_CKM.1/VAU
A_16883	VAU-Protokoll: Aufbau VAUClientHello-Nachricht	FTP_ITC.1/VAU
A_16884	VAU-Protokoll: Nachrichtentypen und HTTP-Content-	FTP_ITC.1/VAU
A_16900	VAU-Protokoll: Client, Behandlung von	FTP_ITC.1/VAU
A_16903	Prüfung der Signatur der VAUServerHelloData	FTP_ITC.1/VAU
A_16941		FTP_ITC.1/VAU
A_16943	VAU-Protokoll: Schlüsselableitung (HKDF)	FCS_CKM.1/VAU
A_16945	VAU-Protokoll: Client, verschlüsselte Kommunikation (1)	FCS_COP.1/VAU
A_16957	VAU-Protokoll: Client, verschlüsselte Kommunikation (2)	FCS_COP.1/VAU
A_17069	VAU-Protokoll: Client Zählerüberlauf	FCS_COP.1/VAU
A_17070	VAU-Protokoll: Aufbau der VAUClientSigFin-Nachricht	FTP_ITC.1/VAU
A_17071	VAU-Protokoll: Versand der VAUClientSigFin-Nachricht	FTP_ITC.1/VAU
A_17074	VAU-Protokoll: Ignorieren von zusätzlichen Datenfeldern in Protokoll-Nachrichten	FTP_ITC.1/VAU
A_17081	VAUProtokoll: zu verwendende Signaturschlüssel	FTP_ITC.1/VAU
A_17084	VAU-Protokoll: Empfang der VAUServerFin-Nachricht	FTP_ITC.1/VAU
A_17094	TLS-Verbindungen Konnektor (ECC-Migration)	Refinement in FTP_ITC.1/NK.TLS

Anforderung aus [90] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-	Ergänzung Anwendungshinweis 87:
A_17206	XML-Signaturen (ECC-Migration)	FDP_DAU.2/AK.QES und FDP_DAU.2/AK.Sig ergänzt.
A_17207	Signaturen binärer Daten (ECC-Migration)	FDP_DAU.2/AK.QES und FDP_DAU.2/AK.Sig ergänzt.
A_17208	Signaturen von PDF/A-Dokumenten (ECC-Migration)	FDP_DAU.2/AK.QES und FDP_DAU.2/AK.Sig ergänzt.
A_17209	Signaturverfahren für externe Authentisierung	FDP_ACF.1/AK.Sgen
A_17210	Konnektor, IKE-Schlüsselaushandlung Fallback	Anmerkung zu FCS_COP.1/NK.Auth ergänzt.
A_17220	Verschlüsselung binärer Daten (ECIES)	Ergänzung FCS_COP.1/AK.CMS.Ent und FCS_COP.1/AK.CMS.Ver
A_17221	XML-Verschlüsselung (ECIES) (ECC-Migration)	Ergänzung FCS_COP.1/AK.XML.Ent und FCS_COP.1/AK.XML.Ver
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen	FTP_ITC.1/NK.TLS
A_17359	Signaturen binärer Daten (Dokumente)	Ergänzung Anwendungshinweis 133: und Anwendungshinweis 134:
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	Ergänzung Anwendungshinweis 132: und Anwendungshinweis 135:
A_17874	SGD-Client, Client-authentisiertes ECIES-Schlüsselpaar	FCS_CKM.1/SGD.ECIES und FCS_COP.1/SGD.ECIES
A_17875	ECIES-verschlüsselter Nachrichtenversand zwischen SGD-Client und SGD-HSM	FCS_COP.1/SGD.ECIES
A_18004	Vorgaben für die Kodierung von Chiffraten (innerhalb von ePA)	FCS_COP.1/VAU
A_18464	TLS-Verbindungen, nicht Version 1.1	Anwendungshinweis 113:und Refinement zu FTP_ITC.1/NK.TLS
A_18467	TLS-Verbindungen, Version 1.3	Wird vom EVG nicht unterstützt.
A_18624	Konnektor, IPsec/IKE: optionale ECC-Unterstützung	EVG unterstützt ECC-Verfahren im Kontext IKE nicht.
A_17688	Nutzung des ECC-RSA-Vertrauensraumes	Ergänzung Anwendungshinweis 87:
A_17690	Nutzung der Hash-Datei für TSL	FPT_TDC.1/NK.Zert
A_17821	Wechsel des Vertrauensraumes bei ECC Migration	Ergänzung Anwendungshinweis 87:
A_17847	Prüfung eines SGD-HSM-Zertifikats (1/2)	FPT_TDC.1/SGD.Zert
A_17848	Prüfung eines SGD-HSM-Zertifikats (2/2)	FPT_TDC.1/SGD.Zert
A_17888	SGD, KeyDerivation (Client)	FTP_ITC.1/SGD
A_17892	Aufwärtskompatibilität JSON-Requests und -Responses	FTP_ITC.1/SGD
A_17897	SGD-Client, Anfrage GetPublicKey (Client)	FTP_ITC.1/SGD
A_17899	SGD-Clients, Auswertung der Kodierung des öffentlichen ECIES- Schlüssels eines SGD-HSMs	FTP_ITC.1/SGD
A_17900	SGD-Clients, Kodierung des eigenen kurzlebigen ECIES-Schlüssels	FTP_ITC.1/SGD
A_17901	SGD-Clients, Kodierung der Signatur des eigenen ECIES-Schlüssels	FTP_ITC.1/SGD
A_17902	Kontext SGD, Chiffrat-Kodierung beim Nachrichtentransport	FTP_ITC.1/SGD

Anforderung aus [90] i.V.m. [93]	Inhaltlicher Abriss der Anforderung	Umsetzung im vorliegenden Security Target
A_17903	Kontext SGD, Prüfung der ephemeren ECC-	FTP_ITC.1/SGD
A_17924	Anfragen an das SGD-HSM (Client)	FTP_ITC.1/SGD
A_17930	interoperables Austauschformat Schlüsselableitungsfunktionalität ePA	FTP_ITC.1/SGD
A_18003	SGD-Client, Prüfung der Telematik-ID bei Berechtigungsvergabe	FTP_ITC.1/SGD
A_18005	SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars	FCS_COP.1/SGD.ECIES, Hinweis 4
A_18006	SGD-Client, KVNR	FTP_ITC.1/SGD
A_18024	SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel	FTP_ITC.1/SGD
A_18025-01	SGD-Client, Anfrage GetAuthenticationToken	FTP_ITC.1/SGD
A_18028	SGD-Client, Auswertung der Anfrage	FTP_ITC.1/SGD
A_18029	SGD-Client, Anfrage KeyDerivation	FTP_ITC.1/SGD
A_18031	SGD-Client, Auswertung der Anfrage KeyDerivation	FTP_ITC.1/SGD
A_20977	SGD-Client, Auswertung der Anfrage KeyDerivation (2/2)	FTP_ITC.1/SGD
A_18032	SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar	FCS_CKM.1/SGD.ECIES
A_15892	FM ePA: Verwendung des Signaturdienstes	FCS_COP.1/AK.XML.SigPr und FCS_COP.1/AK.XML.Sign

Tabelle 36: Über BSI-CC-PP-0098-V3 und PTV3 hinausgehende Anforderungen an die CC-Evaluierung des Konnektors in PTV4

8.4. Anforderungen resultierend aus der Unterstützung des Fachmoduls ePA

Der RISE Konnektor V5.0 unterstützt neben den o.g. Fachmodulen das Fachmodul ePA. Entsprechend der Technischen Richtlinie TR-03157 ([84]), Kapitel 3.2.2, gelten Anforderungen an den Konnektor, die im Rahmen der Evaluierung betrachtet werden müssen. Diese werden im Folgenden zusammengefasst.

Der Anwendungskonnektor stellt dem Fachmodulen ePA bestimmte Funktionen der Basisdienste zur Verfügung, die von den Fachmodulen über entsprechende Schnittstellen zum Konnektor aufgerufen werden können. In Tabelle 37 werden die nach TR-03157 sicherheitsrelevanten Funktionen der Basisdienste anhand der in [93] definierten Technical Use Cases (TUC) aufgelistet und die jeweilige dem Fachmodul angebotene Schnittstelle angegeben.

Dienst	TUC nach [93]	Konnektor-Schnittstelle zum Fachmodul
Zugriffsberechtigungsdienst	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Siehe [RISE-KON-SGFM], Abschnitt 4
Kartendienst	TUC_KON_005 „Card-to-Card authentisieren“	Siehe [RISE-KON-SGFM], Abschnitt 4
Kartendienst	TUC_KON_012 „PIN verifizieren“	Siehe [RISE-KON-SGFM], Abschnitt 4

Kartendienst	TUC_KON_018 „eGK-Sperrung prüfen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Kartendienst	TUC_KON_022 „Liefere PIN-Status“	Siehe [RISE-KON-SGFM], Abschnitt 4
Kartendienst	TUC_KON_026 „Liefere CardSession“	Siehe [RISE-KON-SGFM], Abschnitt 4
Kartendienst	TUC_KON_023 „Karte reservieren“	Dieser TUC wird zwar von der TR ePA, Abschnitt 3.3.2 gefordert, ist jedoch weder von [gemSpec_FM_ePA] gefordert noch vom EVG umgesetzt oder vom FM ePA verwendet.
Kartenterminaldienst	TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	Siehe [RISE-KON-SGFM], Abschnitt 4
Systeminformationsdienst	TUC_KON_254 "Liefere Ressourcendetails"	Siehe [RISE-KON-SGFM], Abschnitt 4
Für Schlüsselerzeugung	TUC_KON_072 „Daten symmetrisch verschlüsseln“ ODER alternativ interne Schnittstelle für Erzeugung eines Akten-, Kontext-, Dokumenten-Schlüssels	Siehe [RISE-KON-SGFM], Abschnitt 4
Signaturdienst	TUC_KON_160 „Dokumente nonQES signieren“	Siehe [RISE-KON-SGFM], Abschnitt 4
TLS-Dienst	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen"	Siehe [RISE-KON-SGFM], Abschnitt 4
TSL-Dienst	TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Verschlüsselungsdienst	TUC_KON_075 „Symmetrisch verschlüsseln“	Siehe [RISE-KON-SGFM], Abschnitt 4
Verschlüsselungsdienst	TUC_KON_076 „Symmetrisch entschlüsseln“	Siehe [RISE-KON-SGFM], Abschnitt 4
Protokollierungsdienst	TUC_KON_271 „Schreibe Protokolleintrag“	Siehe [RISE-KON-SGFM], Abschnitt 4
Zeitdienst	TUC_KON_351 „Liefere Systemzeit“	Siehe [RISE-KON-SGFM], Abschnitt 4
Zertifikatsdienst	TUC_KON_037 „Zertifikat prüfen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Zertifikatsdienst	TUC_KON_034 „Zertifikatsinformationen extrahieren”	Siehe [RISE-KON-SGFM], Abschnitt 4

Namensdienst	TUC_KON_361 „DNS-Namen auflösen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Namensdienst	TUC_KON_362 „Liste der Dienste abrufen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Namensdienst	TUC_KON_363 „Dienstdetails abrufen“	Siehe [RISE-KON-SGFM], Abschnitt 4
Für leichtgewichtige Sicherungs-schicht	Interne Schnittstellen zum Client für leichtgewichtige Sicherungsschicht auf Anwendungsebene	Siehe [RISE-KON-SGFM], Abschnitt 4
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 A_18165 - FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit einem SGD)	Siehe [RISE-KON-SGFM], Abschnitt 4

Tabelle 37: Sicherheitsrelevante Schnittstellen für dasFachmodul ePA

Die korrekte Nutzung der Schnittstellen durch die Fachmodule ist Gegenstand der TR-Zertifizierung nach der Technischen Richtlinie TR-03157. Im Rahmen der CC-Zertifizierung wird die korrekte und sichere Umsetzung der Funktionalität durch den Konnektor geprüft, siehe dazu auch Abschnitt 6.4.5.

Darüber hinaus werden in den Technischen Richtlinien der Fachmodule weitere Sicherheitsanforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung betrachtet werden müssen. Diese werden in der folgenden Tabelle behandelt:

Anforderungen aus TR	**Umsetzung durch den Konnektor**
Rollenprüfung im TLS-Dienst: Das Fachmodul 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.	Refinement zu FTP_ITC.1/VAU
Rollenprüfung in der Basisfunktionalität ‚leichtgewichtige Sicherungsschicht zur VAU‘: Weist das Zertifikat der VAU nicht die Rolle oid_epa_vau auf, MUSS der Konnektor die Verbindung abbrechen.	Refinement zu FTP_ITC.1/VAU

Tabelle 38: Weitere Anforderungen an den Konnektor induziert durch die Technischen Richtlinien für das Fachmodul ePA

8.5. Anforderungen resultierend aus der Produkttypversion 5

Das Protection Profile BSI-CC-PP-0098-V3, das diesem Security Target zugrunde liegt, erfasst alle Sicherheitsanforderungen, die für Produkttypversion 2 (vgl. [88]) des Konnektors

vorgesehen sind. Vorliegender EVG realisiert jedoch bereits Produkttypversion 5 (vgl. [90]) und hat entsprechend [91 und [93] über das Protection Profile und die oben genannten Anforderungen aus Produkttypversion 4 hinausgehende Sicherheitseigenschaften im Rahmen der CC-Evaluierung nachzuweisen. Die folgende Tabelle erfasst diese zusätzlichen Sicherheitseigenschaften (zusätzlich zu Produkttypversion 4) und gibt eine Erläuerung, wie diese im vorliegenden Security Target erfasst sind.

Anforderung aus [91] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
A_17124	TLS-Verbindungen (ECC-Migration)	Umgesetzt nur für TLS Verbindungen, die keine Karten-Kryptographie verwenden. Operation in FDP_ACC.1/NK.Update ergänzt; Refinement zu FTP_ITC.1/NK.TLS angepasst und Anwendungshinweis 113: ergänz
A_19052	Vorgaben für Dokumentformate und Nachrichten	Anwendungshinweis 137: und Anwendungshinweis 134: ergänzt inkl. der dort genannten Ausnahmen. Im Kontext der Ver- und Entschlüsselung nicht umgesetzt
A_18686-01	Komfortsignatur-Timer	Ergänzung Operationen in FDP_ACC.1/AK.Sgen
A_19100	Komfortsignatur-Zähler	Ergänzung Operationen in FDP_ACC.1/AK.Sgen
A_19101	Handbuch-Hinweis zu Nutzerauthentisierung am Clientsystem bei Komfortsignatur	Wird im Benutzerhandbuch umgesetzt.
A_19102-03	TUC_KON_158 „Komfortsignaturen erstellen“	Ergänzung Operationen in FDP_ACC.1/AK.Sgen
A_19103-05	TUC_KON_170 "Dokumente mit Komfort signieren"	Ergänzung in FDP_ACF.1/AK.Sgen Schritt 7 und Ergänzung Operationen in FDP_ACC.1/AK.Sgen
A_19104-03	TUC_KON_171 „Komfortsignatur einschalten“	Ergänzung in FDP_ACF.1/AK.Sgen Schritt 7
A_19105	TUC_KON_172 „Komfortsignatur ausschalten“	Ergänzung Operationen in FDP_ACC.1/AK.Sgen
A_19258	Secure Messaging bei Komfortsignatur	Anwendungshinweis 151: ergänzt
A_19738	Optionaler Import von Konfigurationsdaten durch lokalen Administrator	Optionale Anforderung wird durch den EVG nicht umgesetzt
A_19945	Unterstützte Signaturvarianten bei Komfortsignatur	Anwendungshinweis 160: ergänzt.
A_19971	SGD und SGD-Client, Hashfunktion für Signaturerstellung und -prüfung	Refinement zu FTP_ITC.1/SGD angepasst.
A_20073-01	Prüfung der Länge der UserId	Ergänzung in FDP_ACF.1/AK.Sgen Punkt 3d
A_20074	UserId über 1.000 Vorgänge eindeutig	Ergänzung in FDP_ACF.1/AK.Sgen Punkt 3d
A_21185	Prüfung der detached Signatur der TSL bei Download aus dem Internet	Anwendungshinweis 89: ergänzt.
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	Anwendungshinweis 113: ergänzt.
A_21697	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	Wird in PTV5 des EVG nicht umgesetzt.

Anforderung aus [91] i.V.m. [93]	**Inhaltlicher Abriss der Anforderung**	**Umsetzung im vorliegenden Security Target**
A_21698	Importiertes Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Wird in PTV5 des EVG nicht umgesetzt.
A_21699	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	Wird in PTV5 des EVG nicht umgesetzt.
A_21701	X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen exportieren	Wird in PTV5 des EVG nicht umgesetzt.
A_21702	Intern generierte Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Wird in PTV5 des EVG nicht umgesetzt.
A_21759	Erneuerte ID.AK.AUT für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Wird in PTV5 des EVG nicht umgesetzt.
A_21760	ID.AK.AUT auf gSMC-K für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	Wird in PTV5 des EVG nicht umgesetzt.
TIP1-A_4524-02	Änderung Regel 9	Ergänzung in Ergänzung in FDP_ACF.1/AK.Sgen Punkt 3c
TIP1-A_4561-02	Terminal-Anzeigen für PIN-Operationen	Für ST zu detaillierte Anforderung
TIP1-A_4680-02	Konfigurationswerte des Signaturdienstes	Ergänzung Anwendungshinweis 194:
TIP1-A_4693-02	TUC_KON_032 „TSL aktualisieren”	Anwendungshinweis 89: ergänzt
TIP1-A_4736-02	Kommunikation mit dem Internet (via IAG)	FDP_IFF.1.2/NK.PF ergänzt

Tabelle 39: Über BSI-CC-PP-0098-V3 und PTV4 hinausgehende Anforderungen an die CC-Evaluierung des Konnektors in PTV5

9. Anhang

9.1. Auszüge aus der Konnektorspezifikation [92] zum Zugriffsberechtigungsdienst

Die Inhalte, die in diesem Abschnitt dargestellt werden, sind der Spezifikation Konnektor [gemSpec_Kon] [92], Abschnitt 4.1.1, entnommen. Diese Inhalte bilden die Grundlage der Infomodell-SFP und werden in den entsprechenden funktionalen Sicherheitsanforderungen des Anwendungskonnektors referenziert, insbesondere im Abschnitt 6.3.3.1.

Entität	persistent/ transient	Identitäts -schlüssel	Beschreibung
Mandant	persistent	mandantId	Zu Mandanten und Mandantenfähigkeit siehe Kapitel Mandantenfähigkeit.
Clientsystem	persistent	clientSystemId	Unter einem Clientsystem wird hier ein einzelnes oder eine Gruppe von Systemen verstanden, welche im LAN der Einsatzumgebung auf die Clientsystem-Schnittstelle des Konnektors zugreifen.
CS-AuthMerkmal (CS-AuthProperty)	persistent	csAuthId	Das Authentifizierungsmerkmal dient der Authentifizierung, wenn sich das Clientsystem gegenüber dem Konnektor authentisiert. Der Identitätsschlüssel csAuthId wird bei der Administration vergeben
Arbeitsplatz (Workplace)	persistent	workplaceId	alle dem Konnektor bekannten Arbeitsplätze
Kartenterminal (CardTerminal)	persistent	ctId	alle dem Konnektor bekannten Kartenterminals.
KT-Slot (CT-Slot)	persistent	ctId, slotNo	Die sich in den Kartenterminals befindenden Chipkartenslots (Functional Unit Type 00)
Karte (Card)	transient	cardHandle oder iccsn	Die in den Kartenterminals steckenden Smartcards des Gesundheitswesens, die persönliche Identitäten oder Rollen repräsentieren (eGK, HBA, SMC-B). Karten, die nur Geräteidentitäten tragen (gSMC-K, gSMC-KT) werden in diesem Modell nicht betrachtet. Karten im Sinne dieses Informationsmodells existieren maximal so lange, wie sie im Kartenterminal stecken. Die aktuell im System steckenden Karten werden vom Clientsystem über das cardHandle adressiert. Die iccsn erlaubt eine dauerhafte Adressierung einer Karte.

Entität	persistent/ transient	Identitäts -schlüssel	Beschreibung
			Für den Kartentyp „SM-B“ kann hier auch eine in einem HSM-B enthaltene virtuelle SMC-B abgebildet werden.
Kartensitzung (CardSession)	transient	siehe konkrete Kartensitzungen	Kartensitzungen stellen ein wesentliches Konzept im Sicherheitsmodell des Konnektors dar. Eine Kartensitzung verwaltet einen aktuellen logischen Sicherheitsstatus einer Karte. Die Kartensitzungen sind einer Karte fest zugewiesen. Zu einer Karte kann es mehrere Kartensitzungen geben, die voneinander logisch unabhängige Sicherheitsstatus einer Karte verwalten. Der Konnektor führt alle Zugriffe auf eine Karte im Kontext einer Kartensitzung zu dieser Karte aus. Das Attribut logischerKanal bezeichnet den logischen Kanal zur Karte, der im Rahmen der Kartensitzung verwendet wird.
Kartensitzung_eGK (CardSession_eGK)	transient	cardHandle	Kartensitzung für eine eGK. Die KVK ist im Modell nicht explizit dargestellt. Soweit anwendbar, gelten für die KVK die gleichen Aussagen wie für die eGK.
Kartensitzung_SM-B (CardSession_SM-B)	transient	cardHandle, mandantId	Kartensitzung für eine SM-B
Kartensitzung_HBAx (CardSession_HBAx)	transient	cardHandle, clientSystemId, userId	Kartensitzung für einen HBAx. Unter dem Typ „HBAx“ sind auch die Vorläuferkarten wie „HBA-qSig” und ”ZOD_2.0” inkludiert.
SM-B_Verwaltet (SM-B_managed)	persistent	iccsn	SM-Bs müssen im Gegensatz zu den übrigen Karten im Konnektor vor ihrer Verwendung persistent im Informationsmodell als „SM-B_Verwaltet“ per Administration aufgenommen werden. Dies gilt auch für die in einem HSM-B enthaltenen virtuellen SMC-Bs.
CS_AP	persistent	mandantId, clientSystemId, workplaceId	CS_AP legt die von einem Clientsystem pro Mandanten nutzbaren Arbeitsplätze fest. Ein Clientsystem kann dabei mehrere Arbeitsplätze bedienen. Ebenso können Arbeitsplätze von mehreren Clientsystemen, auch gleichzeitig, genutzt werden, z. B. bei

Entität	persistent/ transient	Identitäts -schlüssel	Beschreibung
			zwei unterschiedlichen, voneinander unabhängigen Praxisprogrammen.
Remote-PIN-KT	persistent	mandantId, workplaceId, ctId	Remote-PIN-KT legt pro Mandant und Arbeitsplatz fest, über welches Kartenterminal eine Remote PIN-Eingabe erfolgen soll, wenn an diesem Arbeitsplatz die PIN-Eingabe für eine Karte erforderlich ist, die nicht in einem dem Arbeitsplatz lokal zugeordneten Kartenterminal steckt.
AuthState	transient	cardHandle, (clientSystemId), (userId), ref	Zu einer Kartensitzung gibt es höhere AuthorizationStates, die durch (type =C2C) Freischaltung oder durch PIN-Eingabe (type=CHV) erreicht werden können.

Tabelle 40: TAB_KON_507 Informationsmodell Entitäten aus [92]

Attribut	Beschreibung
cardHandle	Das Identifikationsmerkmal einer Karte für die Dauer eines Steckzyklusses. Es wird mit dem Entfernen der Karte aus dem Kartenterminal ungültig. Es wird automatisch vom Konnektor vergeben.
clientSystemId	Das Identifikationsmerkmal eines Clientsystems. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.
csAuthId	Das Identifikationsmerkmal eines Authentifizierungsmerkmals.
ctId	Das Identifikationsmerkmal eines Terminals. Es ist eine fixe Eigenschaft des Kartenterminals.
iccsn	Die Seriennummer einer Karte. Sie identifiziert eine Karte dauerhaft.
isHSM	Attribut der Entitäten Karte und SM-B_Verwaltet. Es ist false, wenn eine echte Smardcard abgebildet wird und true, wenn es sich um eine virtuelle SMC-B handelt, die in einem HSM-B enthalten ist.
isPhysical	Attribut des Kartenterminals das den Wert „Ja“ hat, wenn es sich um ein tatsächlich existierendes Kartenterminal handelt. Ist der Wert „Nein“, dann handelt es sich um ein logisches Kartenterminal im Zusammenhang mit einem HSM-B.
logicalChannel	Referenz auf ein Objekt, das einen logischen Kanal repräsentiert.
mandantId	Das Identifikationsmerkmal eines Mandanten. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.

Attribut	Beschreibung
ref	Das Identifikationsmerkmal eines AuthState zu einer gegebenen Kartensitzung. Im Falle C2C handelt es sich um die KeyRef (mit einer bestimmten Rolle) und in Falle CHV um eine referenzierte PIN.
slotNo	Das Identifikationsmerkmal eines Slot für ein bestimmtes Kartenterminal. Diese fortlaufende Nummer ist eine fixe Eigenschaft des Kartenterminals. Sie beginnt bei 1.
type	Als Kartenattribut: Typ einer Karte. Im Folgenden berücksichtigte Werte: „HBAx“, „SM-B“, „EGK“. Als Attribute eines AuthState: Typ des AuthState. „C2C“ steht für gegenseitige Kartenauthentisierung. „CHV“ steht für Card Holder Verification per PIN-Eingabe.
userId	Das Identifikationsmerkmal des Nutzers im Clientsystem (Die userId wird durch das Clientsystem vergeben und verwaltet). Die userId wird im Kontext eine Kartensitzung_HBAx vom Konnektor verwendet, um als Bestandteil des Identitätsschlüssels die Kartensitzung_HBAx zu identifizieren.
workplaceId	Das Identifikationsmerkmal eines Arbeitsplatzes. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.

Tabelle 41: TAB_KON_508 Informationsmodell Attribute aus [92]

Entitätenbeziehung	persistent/ transient	Beschreibung
Authentifikationsmerkmale des Clientsystems [1]	persistent	Diese Relation legt für jedes Clientsystem eine Menge von Authentisierungsmerkmalen fest. Mit einem dieser Authentisierungsmerkmale muss sich ein Client gegenüber dem Konnektor authentisiert haben, um als das entsprechende Clientsystem vom Konnektor akzeptiert zu werden.
Clientsysteme des Mandanten [2]	persistent	Diese Relation weist Clientsystemen Mandanten zu.
Arbeitsplätze des Mandanten [3]	persistent	Diese Relation weist Arbeitsplätze Mandanten zu. Arbeitsplätze können von mehreren Mandanten genutzt werden. Z. B. kann ein von mehreren Mandanten genutzter gemeinsamer Empfang als ein Arbeitsplatz modelliert werden.
Kartenterminals des Mandanten [5]	persistent	Diese Relation weist Kartenterminals Mandanten zu.

Entitätenbeziehung	persistent/ transient	Beschreibung
Lokale Kartenterminals [6]	persistent	Diese Relation erfasst die Kartenterminals, die sich lokal an einem Arbeitsplatz befinden und von diesem genutzt werden können. Die Modellierung lässt es zu, dass Kartenterminals mehreren Arbeitsplätzen lokal zugewiesen werden. Jeder an der TI teilnehmende Arbeitsplatz wird in der Regel mindestens ein lokales Kartenterminal benötigen.
Entfernte Kartenterminals [7]	persistent	Diese Relation beschreibt, auf welche Kartenterminals Arbeitsplätze (remote) zugreifen dürfen. Dies ist für zentral steckende Karten vorgesehen.
Slot eines Kartenterminals [8]	persistent	Die Zuordnung von Slots zu einem Kartenterminal ergibt sich automatisch aus den Eigenschaften des Kartenterminals.
SM-B_Verwaltet eines Mandanten [9]	persistent	Diese Relation legt fest, welche verwalteten SM-Bs einem Mandanten zugeordnet sind.
Kartenterminal-Slot, in dem eine Karte steckt [10]	transient	Sobald eine Karte in ein Kartenterminal gesteckt wird, ergibt sich implizit eine Relation der Karte zu dem Slot, in dem sie steckt, [6] und indirekt über [4] zum Kartenterminal.
Mandant der Kartensitzung SM-B [11]	transient	Beim Anlegen einer Kartensitzung SM-B wird diese immer dem zugreifenden Mandanten zugeordnet.
Arbeitsplatz der Kartensitzung eGK [12]	transient	Eine Kartensitzung eGK ist immer einem Arbeitsplatz zugeordnet.
Karte einer Kartensitzung [13]	transient	Jeder Kartensitzung ist genau einer Karte zugeordnet.
Gesteckte SM-B [14]	transient	Wird eine SM-B gesteckt und handelt es sich um eine verwaltete SM-B, ergibt sich über die iccsn die Zuordnung.
Freischaltung einer Karte [15]	transient	Diese Relation erfasst die Freischaltung einer Karte durch eine andere Karte.
Bindung der Kartensitzung_HBAx an Clientsystem [16]	transient	Kartensitzungen HBAx sind einem Clientsystem zugeordnet.
AuthState pro Kartensitzung [17]	transient	Eine Kartensitzung kann erhöhte Sicherheitszustände (Authorization State) haben.

Tabelle 42: TAB_KON_509 Informationsmodell Entitätenbeziehungen aus [92]

#	Beschreibung	Definition mittels OCL[325]
C1	Eine eGK muss eine oder keine Kartensitzung haben.	**context** Karte **inv:** self.type = "eGK" implies self.kartensitzung.size() <= 1
C2	Wenn zwei Kartensitzungen einer HBAx dem gleichen Clientsystem zugeordnet sind und ihre userIds gleich sind, dann müssen die beiden Kartensitzungen identisch sein.	**context** Kartensitzung-HBAx **inv:** forAll(k1, k2 : Kartensitzung-HBAx | k1.karte = k2.karte and k1.clientsystem = k2.clientsystem and k1.userId = k2.userId implies k1 = k2)
C3	Wenn zwei SM-B-Kartensitzungen einer Karte dem gleichen Mandanten zugeordnet sind, dann müssen die beiden Kartensitzungen identisch sein.	**context** Kartensitzung-SM-B **inv:** forAll(k1, k2 : Kartensitzung-SM-B | k1.karte = k2.karte and k1.mandant = k2.mandant implies k1 = k2)
C4	Die Seriennummer iccsn einer Karte muss eindeutig sein.	**context** Karte **inv:** Karte.allInstances -> isUnique(iccsn)
C5	Die Seriennummer iccsn einer Karte muss für die vom Konnektor verwalteten SM-Bs eindeutig sein.	**context** SM-B_Verwaltet **inv:** SM-B_Verwaltet.allInstances -> isUnique(iccsn)
C6	Das CardHandle einer Karte muss eindeutig sein.	**context** Karte **inv:** Karte.allInstances -> isUnique(cardHandle)
C7	Die Identifikationsnummer des Clientsystems muss eindeutig sein.	**context** Clientsystem **inv:** Clientsystem.allInstances -> isUnique(clientSystemId)
C8	Die Identifikationsnummer des Mandanten muss eindeutig sein.	**context** Mandant **inv:** Mandant.allInstances -> isUnique(mandantId)
C9	Die Identifikationsnummer des Arbeitsplatzes muss eindeutig sein.	**context** Arbeitsplatz **inv:** Arbeitsplatz.allInstances -> isUnique(workplaceId)
C10	Die Identifikationsnummer des Kartenterminals muss eindeutig sein.	**context** Kartenterminal **inv:** Kartenterminal.allInstances -> isUnique(ctId)

[325] Die Constraints werden im UML ergänzenden Standard OCL definiert.

#	Beschreibung	Definition mittels OCL[325]
C11	Die Identifikationsnummer (slotNo) des Kartenterminal-Slots für ein gegebenes Kartenterminal muss eindeutig sein.	**context** Kartenterminal **inv:** self.kT-Slot -> isUnique(slotNo)
C12	Es muss gewährleistet sein, dass nur Arbeitsplätze und Clientsysteme einander im Rahmen eines Mandanten zugeordnet werden, die diesem Mandanten selbst zugeordnet sind.	**context** CS-AP **inv:** self.arbeitsplatz.mandant.includes(self.mandant) **inv:** self.clientsystem.mandant.includes(self.mandant)
C13	Es muss gewährleistet sein, dass nur Kartenterminals und Arbeitsplätze einander im Rahmen eines Mandanten zur Remote-PIN-Eingabe zugeordnet werden, die diesem Mandanten selbst zugeordnet sind.	**context** Remote-PIN-KT **inv:** self.arbeitsplatz.mandant.includes(self.mandant) **inv:** self.kartenterminal.mandant.includes(self.mandant)
C14	Zur Remote-PIN-Eingabe muss ein lokales Kartenterminal ausgewählt sein.	**context** Remote-PIN-KT **inv:** self.arbeitsplatz.localKartenterminal.includes(self.kartenterminal) **inv:** not self.arbeitsplatz.entferntKartenterminal.includes(self.kartenterminal)
C15	Zur Remote-PIN-Eingabe darf pro Mandanten und Arbeitsplatz nicht mehr als ein Kartenterminal ausgewählt werden.	**context** Remote-PIN-KT **inv:** forAll(r1, r2 : Remote-PIN-KT | r1.arbeitsplatz = r2.arbeitsplatz and r1.mandant = r2.mandant implies r1 = r2)
C16	Eine Kartensitzung-HBAx muss immer eine zugehörige userId haben.	**context** Kartensitzung-HBAx **inv:** self.userId <> null

Tabelle 43: TAB_KON_510 Informationsmodell Constraints aus [92]

Element	Beschreibung
Name	TUC_KON_000 ”Prüfe Zugriffsberechtigung”
Beschreibung	Es wird geprüft, ob eine Autorisierung im Rahmen der angegebenen Eingangsdaten erteilt wird.
Eingangs-anforderungen	keine
Auslöser und Vorbedingungen	Aufruf einer Operation des Konnektors durch das Clientsystem.

Element	Beschreibung
Eingangsdaten	• mandantId • clientSystemId • workplaceId • userId (optional) • ctId (optional) • cardHandle (optional) • needCardSession (needCardSession=true; doNotNeedCardSession=false; default: true; optional; wenn der Parameter leer ist, gilt der Default-Wert) Verwendet der aufrufende TUC eine Kartensitzung ist der Wert true, verwendet er keine Kartensitzung ist der Wert false. Die Berechtigungsprüfung geht im Default-Fall, davon aus, dass eine Kartensitzung benötigt wird, und prüft für diesen Fall die Berechtigung mit. • allWorkplaces (allWorkplaces=true; allWorkplace=false; default: false; optional; wenn der Parameter leer ist, gilt der Default-Wert) Dieser Parameter muss dann (true) gesetzt werden, wenn die Berechtigungsprüfung nicht auf die vom angegebenen Arbeitsplatz erreichbaren Kartenterminals beschränkt ist, sondern sich auf alle vom Clientsystem(clientSystemId) und dem Mandant (mandantId) insgesamt erreichbaren Kartenterminals beziehen soll. Ist dieser Schalter gleich true, wird die Berechtigung unabhängig vom Eingangsparameter workplaceId geprüft.
Komponenten	Konnektor
Ausgangsdaten	• keine (Autorisierung erteilt) • Fehler (Autorisierung nicht erteilt, siehe technische Fehlermeldung)
Standardablauf	1. Prüfe, ob die Pflichtparameter (mandantId, clientSystemId, workplaceId) vollständig gesetzt sind. 2. Falls ANCL_CAUT_MANDATORY = Enabled, dann prüfe, ob die gemäß [TIP1-A_4516] durchgeführte Authentifizierung über ein dem Clientsystem zugeordnetes CS-AuthMerkmal erfolgte. 3. Ermittle Zugriffsregel R zu den Aufrufparametern: 3.1. Falls der Parameter cardHandle nicht null ist, muss das Kartenobjekt des Informationsmodells Karte(cardHandle) ermittelt werden. 3.2. Zu den Parametern (ctId, cardHandle, needCardSession, allWorkplaces) muss mittels Tabelle „TAB_KON_513 Zugriffsregeln Regelzuordnung“ die Zugriffsregel R ermittelt werden. 4. Prüfe die Bedingungen der in Schritt 3 ermittelten Regel R: 4.1. Zur Regel R muss die relevante Spalte in Tabelle „TAB_KON_514 Zugriffsregeln Definition“ ermittelt werden. 4.2. Jede Zeile, die in der Spalte R ein „x“ hat, muss geprüft werden: 4.2.1. Prüfe, ob die in Spalte „Bedingung“ mittels OCL formulierte Bedingung für die Eingangsdaten erfüllt ist.

Element	Beschreibung
Varianten/ Alternativen	Bei einem Aufruf mit einem cardHandle zu den Kartentypen SMC-KT und UNKNOWN wird Schritt 3 in folgender Variante durchlaufen: (4) Ermittle Zugriffsregel R zu den Aufrufparametern: 4.1. ctId wird zum cardHandle bestimmt 3.2. Zu den Parametern (ctId, cardHandle: null, needCardSession: false, allWorkplaces: false) muss mittels Tabelle „TAB_KON_513 Zugriffsregeln Regelzuordnung“ die Zugriffsregel R ermittelt werden.
Fehlerfälle	Fehler im Ablauf (Standardablauf oder Varianten) führen in den folgend ausgewiesenen Schritten zu einem Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes: (→1) Es sind nicht alle Pflichtparameter gesetzt, Fehlercode: 4021 (→2.) Clientsystem aus dem Aufrufkontext nicht authentifiziert, Fehlercode: 4204 (→3.1) Karte nicht als gesteckt identifiziert, Fehlercode: 4008 (→3.2) Zu den Parametern konnte keine Regel ermittelt werden, Fehlercode: 4019 (→4.2.1) Bedingung nicht erfüllt Fehlercode: wie in Spalte „ErrorCode“ der geprüften Zeile aus Tabelle „TAB_KON_514 Zugriffsregeln Definition“
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	PIC_KON_118 Aktivitätsdiagramm zu „TUC_KON_000 Prüfe Zugriffsberechtigung“

Tabelle 44: TAB_KON_511 - TUC_KON_000 „Prüfe Zugriffsberechtigung“ aus [92]

Regel	Beschreibung
R1	Innerhalb des Mandanten m darf das Clientsystem cs verwendet werden.
R2	Innerhalb des Mandanten m darf das Clientsystem cs auf das Kartenterminal kt zugreifen.
R3	Innerhalb des Mandanten m darf das Clientsystem cs den Arbeitsplatz ap nutzen.
R4	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf das Kartenterminal kt zugreifen.
R5	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die lokal gesteckte eGK zugreifen. Eine Kartensitzung wird nicht benötigt.
R6	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die lokal gesteckte eGK zugreifen. Eine Kartensitzung wird benötigt. Wenn bereits eine Kartensitzung besteht, ist sichergestellt, dass sie vom Arbeitsplatz ap gestartet wurde.
R7	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die SM-B zugreifen. Es wird dabei sichergestellt, dass es sich um eine im Mandanten verwaltete SM-B handelt.

Regel	Beschreibung
R8	Innerhalb des Mandanten m darf das Clientsystem cs auf den HBAx zugreifen. Eine Kartensitzung wird nicht benötigt.
R9	Innerhalb des Mandanten m darf das Clientsystem cs auf den HBAx zugreifen. Eine Kartensitzung wird benötigt. Wenn bereits Kartensitzungen zum HBAx bestehen, wird der Zugriff auf den HBAx verhindert, wenn es eine Kartensitzung zum selben Clientsystem, aber einer anderen UserId gibt, deren Sicherheitszustand erhöht ist.

Tabelle 45: TAB_KON_512 Zugriffsregeln Beschreibung

Parameter	R1	R2	R3	R4	R5	R6	R7	R8	R9
`ctId`	null	not null	null	not null					
`cardHandle`	null	null	null	null	not null	not null	not null	not null	not null
`Karte(cardHandle).type`					eGK oder KVK	eGK oder KVK			
`Karte(cardHandle).type`							SM-B		
`Karte(cardHandle).type`								HBAx	HBAx
`needCardSession`	false	false	false	false	false	true	true oder false	false	true
`allWorkplaces`	true	true	false	false	false	false	false	false	false

Tabelle 46: TAB_KON_513 Zugriffsregeln Regelzuordnung aus [92]

Bedingung[326]	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
`inv : userId <> null`									x	4003
`let m : Mandant = Mandant(mandantId)` `inv : m <> null`	x	x	x	x	x	x	x	x	x	4004

`let cs : Clientsystem`
`= Clientsystem(clientSystemId)`
`inv : cs <> null`
	x	x	x	x	x	x	x	x	x	4005

`let ap : Arbeitsplatz`
`= Arbeitsplatz(workplaceId)`
`inv : ap <> null`
			x	x	x	x	x	x	x	4006

`let kt : Kartenterminal`		x		x						4007

Entität[327]

[326] Jede Bedingung ist als Constraint mittels OCL definiert, ist einzeln prüfbar und hat als Eingangsparameter mandantId, clientSystemId, workplaceId, ctId, cardHandle und userId.

[327] Zur Bezeichnung einer Objektinstanz, die im Informationsmodell vorhanden ist, wird die Notation <<Entitätsbezeichner>>(<<Komma separierte Liste der Identitätsschlüssel>> verwendet.

	Bedingung[326]	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**Error Code**
	= Kartenterminal(ctId) inv : kt <> null										
	let k : Karte = Karte(cardHandle) inv : k <> null					x	x	x	x	x	4008
Mandantbezug	let m : Mandant = Mandant(mandantId) let cs : Clientsystem = Clientsystem(clientSystemId) inv : cs.mandant.includes(m)	x	x	x	x	x	x	x	x	x	4010
Mandantbezug	let m : Mandant = Mandant(mandantId) let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) inv : ap.mandant.includes(m)			x	x	x	x	x	x	x	4011
Mandantbezug	let m : Mandant = Mandant(mandantId) let kt : Kartenterminal = Kartenterminal(ctId) inv : kt.mandant.includes(m)		x		x						4012
Mandantbezug	let m : Mandant = Mandant(mandantId) let k : Karte = Karte(cardHandle) inv : k.kT-Slot.kartenterminal.mandant .includes(m)					x	x	x	x	x	4012
Relation	let k : Karte = Karte(cardHandle) inv : k.SM-B_Verwaltet <> null							x			4009
Relation	let m : Mandant = Mandant(mandantId) let k : Karte = Karte(cardHandle) inv : k.SM-B_Verwaltet.mandant -> includes(m)							x			4013
Relation	let m : Mandant = Mandant(mandantId) let cs : Clientsystem = Clientsystem(clientSystemId) let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) inv : CS_AP.allInstances -> exists(c : CS_AP | c.mandant = m and c.arbeitsplatz = ap and c.clientsystem = cs)			x	x	x	x	x	x	x	4014
Relation	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let kt : Kartenterminal = Kartenterminal(ctId) inv : ap.lokalKartenterminal.includes(kt) or ap.entferntKartenterminal.includes(kt)				x						4015
Relation	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let kt : Kartenterminal = Karte(cardHandle).kT-Slot.kartenterminal inv :							x	x	x	4015

	Bedingung[326]	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
	ap.lokalKartenterminal.includes(kt) or ap.entferntKartenterminal.includes(kt)										
	let m : Mandant = Mandant(mandantId) let kt : Kartenterminal = Kartenterminal(ctId) let cs : Clientsystem = Clientsystem(clientSystemId) inv : CS_AP.allInstances -> exists(c : CS_AP | c.arbeitsplatz.lokalKartenterminal .includes(kt) or c.arbeitsplatz.entferntKartenterminal .includes(kt) and c.mandant = m and c.arbeitsplatz.mandant.includes(m) and c.clientsystem = cs)		x								4020
	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let kt : Kartenterminal = Karte(cardHandle).kT-Slot.kartenterminal inv : ap.lokalKartenterminal.includes(kt)					x	x				4016
Kartensitzungen	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let k : Karte = Karte(cardHandle) inv : k.kartensitzung -> not exists(ks : Kartensitzung | ks.arbeitsplatz <> ap)						x				4017
	let k : Karte = Karte(cardHandle) let cs : Clientsystem = Clientsystem(clientSystemId) inv : k.kartensitzung -> not exists(ks : Kartensitzung | ks.clientsystem = cs and ks.userId <> userId and ks.authState.size() > 0)									x	4018

Tabelle 47: TAB_KON_514 Zugriffsregeln Definition aus [92]

9.2. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AK	Anwendungskonnektor
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

Abkürzung	Bedeutung
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 to be 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)
HBA	Heilberufsausweis, Englisch: Health Professional Card (HPC)
HBAx	Bezeichnung für Chipkarten des Typs HBA, HBA-qSig und ZOD-2.0
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
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

Abkürzung	Bedeutung
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
S/MIME	Secure / Multipurpose Internet Mail Extensions
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 (Authentisierungsverifikationsdaten 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

Abkürzung	Bedeutung
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.
AMTS	Arzneimitteltherapiesicherheit
NFDM	Notfalldatenmanagement

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.
Anwendungskonnektor	Der Teil des Konnektors [92], 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.
Authentisierungsreferenz-daten	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. [75]).
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.

Begriff	Definition
Kartenhandle (BKH)	Handle zur Identifizierung einer Chipkarte, die in einem eHealth-Kartenterminal steckt. Mit diesem BKH sind folgende Informationen verknüpft (s. [92], 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. [92], 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 Dokument: 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 [8].
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 [94], evaluiert gemäß [80] 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 [8] 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

Begriff	Definition
	eine Chipkarte (PIN-Empfänger) in einem anderen Chipkarten-Terminal unter Steuerung der AK (s. [75], Kap. 2.1.2, und [92], 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 [10], definiert (Abs. (2): Pflichtanwendungen, Abs. (3): freiwillige Anwendungen): • Übermittlung ärztlicher Verordnungen (Verordnungsdatenmanagement, 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 [8] 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:

Begriff	Definition
	Gültige Zertifikate müssen im Zertifikatsverzeichnis des ausstellenden qualifizierter Vertrauensdiensteanbieters vorhanden sein. Der Vertrauensdiensteanbieter ist nach eIDAS [8] 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.
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 [97] und [99], dessen Betriebssystem nach PP COS G2 [79] 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. [92], 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 [92].
Krankenversichertenkarte (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.

Begriff	Definition
Managementschnittstelle	(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 [8] 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 [8] 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 [8] Anhang I erfüllt.
qualifizierter Vertrauens-diensteanbieter	„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 [8] 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. [99], Kap. 9).
qualifizierte elektronische Signaturerstellungseinheit	Konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird und die Anforderungen aus eIDAS [8] Anhang II erfüllt; Abkürzung: QSEE. Englisch:QSCD.
Sicherer PIN-Modus	Tastatureingabemodus des eHealth-Kartenterminals gemäß [94], in dem das eHealth-Kartenterminal durch ein SICCT-Kommando [96] angewiesen wird, die Tastatureingabedaten in einem angegebenen Chipkartenkommando an eine Chipkarte in einem angegebenen Chipkartensteckplatz zu senden und die Antwort

Begriff	Definition
	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. [92], 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 [97] und [100], dessen Betriebssystem nach PP COS G2 [79] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.

Begriff	Definition
SMC Typ KT (gSMC-KT)	Sicherheitsmodul des Kartenterminals. Chipkarte gemäß Spezifikation [97] und [102], dessen Betriebssystem nach PP COS G2 [79] 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 [97] und [101], die durch die gematik zugelassen wurde.
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.
Verschlüsselungsrichtlinie	Verschlüsselungsrichtlinie, die beschreiben • das Verschlüsselungsformat (EncryptionType): Cryptographic Message Syntax [34], XML-Encryption [21] oder S/MIME [35], • 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-

Begriff	Definition
	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.
Vertrauensdiensteanbieter	„Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt, vgl. eIDAS [8] 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 Verschlüsselungsrichtlinie	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.

9.4. Abbildungsverzeichnis

9.5. Tabellenverzeichnis

9.6. Literaturverzeichnis

9.6.1. Kriterien

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

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

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

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

[5] Common Criteria Supporting Document, Mandatory Technical Document, Composite evaluation of Smart Cards and similar devices, September 2007, Version 1.0, Revision 1, CCDB-2007-09-001

[6] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[7] W. Killmann, W. Schindler: A proposal for: Functionality classes for random number generators. Version 2.0, September 2011

9.6.2. Gesetze und Verordnungen

[8] 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

[9] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms Version 1.1 vom Juni 2018

[10] Sozialgesetzbuch, Fünftes Buch (SGB V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 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. Standards

[11] ISO/IEC 8859-15:1998 - 8-bit single-byte coded graphic character sets, Part 15: Latin alphabet No. 9, published March 15, 1999

[12] ISO 19005 – Document management – Electronic document file format for long-term preservation

[13] ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)

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

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

[16] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques. December 2001

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

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

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

[20] Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation 26 November 2008, https://www.w3.org/TR/xml/

[21] XML Encryption Syntax and Processing, Version 1.1 W3C Recommendation, 11 April 2013, https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/

[22] XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[23] XML Path Language (XPath) 2.0 (Second Edition), W3C Recommendation, 14 December 2010, https://www.w3.org/TR/2010/REC-xpath20-20101214/

[24] XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 23 January 2007, https://www.w3.org/TR/2007/REC-xslt20-20070123/

[25] 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/

[26] 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

[27] 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

[28] RFC 1305 (March 1992) Network Time Protocol (Version 3), Specification, Implementation and Analysis, http://www.ietf.org/rfc/rfc1305.txt

[29] J. Burbank, J. Martin, W. Kasch, (September 5, 2008): Network Time Protocol Version 4 Protocol And Algorithms Specification draft-ietf-ntp-ntpv4-proto-11, http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-proto-11

[30] RFC 4330 (Januar 2006): Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, http://www.ietf.org/rfc/rfc4330.txt

[31] 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

[32] RFC 2315 (März 1998): PKCS #7: Cryptographic Message Syntax, Version 1.5, http://www.ietf.org/rfc/rfc2315.txt

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

[34] RFC 5652 (September 2009): Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc5652.txt

[35] RFC 5751 (Januar 2010): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, Message Specification, http://www.ietf.org/rfc/rfc5751.txt (für MIME s. RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049)

[36] 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

[37] 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

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

[39] SEC 1: Elliptic Curve Cryptography, Certicom Research. Version 2.0, 21.05.2009, http://www.secg.org/download/aid-780/sec1-v2.pdf

[40] ECC Brainpool Standard Curves and Curve Generation. Version 1.0, 19.10.2005. http://www.teletrust.de/fileadmin/files/oid/oid_ECC-Brainpool-Standard-curves-V1.pdf

[41] TIFF Revision 6.0, http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

[42] Unicode Standard Version 6.2.0. http://www.unicode.org/versions/Unicode6.2.0/

[43] 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

[44] 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

[45] 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

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

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

[48] 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

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

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

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

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

[53] 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

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

[55] 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

[56] 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

[57] 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

[58] 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

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

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

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

[62] T. Berners-Lee, R. Fielding, L. Masinter: Uniform Resource Identifier (URI): Generic Syntax, RFC 3986, January 2005, https://www.ietf.org/rfc/rfc3986.txt

[63] Cross-Origin Resource Sharing, W3C Recommendation, January 2014, http://www.w3.org/TR/2014/REC-cors-20140116/

[64] W. Polk, R. Housley, L. Bassham: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3279 (April 2001), http://www.ietf.org/rfc/rfc3279.txt

[65] M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639 (March 2010),

[66] R. Housley: Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, RFC 5083, November 2007, https://tools.ietf.org/html/rfc5083

[67] 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

[68] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[69] H. Krawczyk, P. Eronen: HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [RFC 5869], (May 2010), https://tools.ietf.org/html/rfc5869

[70] S. Cantor, J. Kemp, R. Philpott, E. Maler: H. Krawczyk, P. Eronen: Assertions and Protocols for the OASIS Security Assertion Markup Language(SAML) V2.0, OASIS Standard, 15 March 2005, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[71] RFC 5639 (March 2010): Elliptic Curve Cryptography (ECC) Brainpool, Standard Curves and Curve Generation, http://www.ietf.org/rfc/rfc5639.txt

[72] RFC 7027: (October 2013) Elliptic Curve Cryptography (ECC) Brainpool, Curves for Transport Layer Security (TLS), https://tools.ietf.org/html/rfc7027

9.6.4. Schutzprofile (Protection Profiles) und Technische Richtlinien

[73] 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 2014-01

[73a] Update von [73] für OBP1: 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 2017-01

[74] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.0, 28.08.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[75] BSI TR-03114 Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[76] Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.19, 04.12.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[76a] Update von 76: Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20, 21.09.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[77] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097-V2, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.6.5, 12.03.2021

[78] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3, Version 1.5.9 vom 15.04.2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[79] Common Criteria Schutzprofil (Protection Profile) Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-2013, 06.09.2013 und jede darauf angewandte Maintenance und Rezertifizierung, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[80] Protection Profile Electronic Health Card Terminal, BSI-PP-0032, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.7, 21.09.2016

[81] Technische Richtlinie BSI TR-03144, eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.2, 27.07.2017

[82] Technische Richtlinie BSI TR-03154, Konnektor – Prüfspezifikation für das Fachmodul NFDM, Version 1.0.1, 23.05.2018, Bundesamt für Sicherheit in der Informationstechnik

[83] Technische Richtlinie BSI TR-03155, Konnektor – Prüfspezifikation für das Fachmodul AMTS, Version 1.0.1, 23.05.2018, Bundesamt für Sicherheit in der Informationstechnik

[84] Technische Richtlinie BSI TR-03157, Konnektor – Prüfspezifikation für das Fachmodul ePA, Version 2.0, 03.08.2021, Bundesamt für Sicherheit in der Informationstechnik

9.6.5. Spezifikationen

[85] Einführung der Gesundheitskarte: Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP], Version 2.10.0, 02.03.2020, gematik GmbH

[86] Elektronische Gesundheitskarte und Telematikinfrastruktur. Übergreifende Spezifikation. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.16.1, 27.08.2020

[87] Elektronische Gesundheitskarte und Telematikinfrastruktur. Übergreifende Spezifikation. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik GmbH, Version 2.19.1, 30.06.2021

[88] Einführung der Gesundheitskarte: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV2.8.0], Version 2.8.0, 13.02.2017, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[89] Update von [88] für PTV3: Einführung der Gesundheitskarte: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV3_3.3.0-0], Version 1.0.1, 07.11.2018, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[90] Update von [88] für PTV4: Einführung der Gesundheitskarte: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV4_4.7.0-0], Version 1.0.0, 18.09.2020, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[91] Update von [88] für PTV5: Elektronische Gesundheitskarte und Telematikinfrastruktur: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV5_5.0.2-1], Version 1.0.0, 28.10.2021, gematik GmbH

[92] Einführung der Gesundheitskarte: Spezifikation Konnektor, Version 5.9.3, 21.09.2020, gematik GmbH

[93] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Konnektor, Version 5.14.0, 02.09.2021, gematik GmbH

[94] Einführung der Gesundheitskarte. Spezifikation eHealth-Kartenterminal [gemSpec_KT], Version: 3.5.0, Stand: 17.06.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[95] Einführung der Gesundheitskarte: Spezifikation Fachmodul VSDM [gemSpec_FM_VSDM], Version 1.5.0, 26.08.2014 mit Errata zu R1.5.3, Version 1.00

vom 22.09.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[96] 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

[97] Einführung der Gesundheitskarte: Spezifikation des Card Operating System (COS) Elektrische Schnittstelle [gemSpec_COS], Version 3.8.0, 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[98] Einführung der Gesundheitskarte: Spezifikation der elektronischen Gesundheitskarte – eGK-Objektsystem [gemSpec_eGK_ObjSys], Version 3.9.0, 24.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[99] Einführung der Gesundheitskarte: Spezifikation des elektronischen Heilberufsausweises – HBA-Objektsystem [gemSpec_HBA_ObjSys], Version 3.8.1, 30.09.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[100] Einführung der Gesundheitskarte. Spezifikation der Security Module Card SMC-B Objektsystem [gemSpec_SMCB_ObjSys], Version 3.8.0, 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[101] Einführung der Gesundheitskarte: Spezifikation der gSMC-K – Objektsystem [gemSpec_gSMC-K_ObjSys], Version 3.8.0, 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[102] Einführung der Gesundheitskarte. Spezifikation der gSMC-KT – Objektsystem [gemSpec_gSMCKT_ObjSys], Version 3.8.0, 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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

[104] Einführung der Gesundheitskarte. Spezifikation TSL-Dienst [gemSpec_TSL]. Version 1.7.0, Stand 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[105] Einführung der Gesundheitskarte. Spezifikation Verzeichnisdienst [gemSpec_VZD]. Version 1.2.0, Stand 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[106] Einführung der Gesundheitskarte: Übergreifende Spezifikation: Spezifikation Netzwerk [gemSpec_Net], gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 1.6.0, 17.07.2015

[107] UEFI, Unified Extensible Firmware Interface Specification, Version 2.7, May 2017, Unified EFI Forum

[108] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation Fachmodul NFDM [gemSpec_FM_NFDM], gematik GmbH, Version 1.6.2, 30.06.2021

[109] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation Fachmodul AMTS [gemSpec_FM_AMTS], gematik GmbH, Version 1.4.0, 15.05.2019

[110] Signaturrichtlinie QES, Notfalldaten-Management (NFDM) [gemRL_QES_NFDM], gematik GmbH, Version 1.4.1, 02.03.2020

[111] Informationsmodell Notfalldaten-Management (NFDM) [gemSpec_InfoNFDM

[112] Elektronische Gesundheitskarte und Telematikinfrastruktur. Spezifikation Fachmodul ePA [gemSpec_FM_ePA], gematik GmbH, Version 1.9.0, 09.07.2021.

[113] Informationsmodell eMP/AMTS-Datenmanagement [gemSpec_Info_AMTS], gematik GmbH, Version 1.5.0, 02.10.2019

[114] Elektronische Gesundheitskarte und Telematikinfrastruktur: Spezifikation Schlüsselgenerierungsdienst ePA [gemSpec_SGD_ePA], gematik GmbH, Version 1.4.2, 19.02.2021

9.6.6. Weitere Dokumente

Die gültigen Versionen der Dokumente in diesem Abschnitt sind dem Zertifizierungsreport zu entnehmen, der zusammen mit diesen Sicherheitsvorgaben von der Zertifzierungsstelle veröffentlicht wird.

[RISE-KON-AGD_OPE]	RISE Konnektor Operational User Guidance, RISE GmbH
[RISE-KON-SRLRQ]	RISE Konnektor – Signaturrichtlinien, RISE GmbH
[RISE-KON-ITD]	Konzept Integritätsprüfung TSF, RISE GmbH
[RISE-KON-SGFM]	RISE Konnektor Security Guidelines für Fachmodule
[RISE-KON-FSP]	RISE Konnektor - Functional Specification (ADV_FSP)