Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Schutzprofil (Protection Profile)

Schutzprofil 2:
Anforderungen an den Konnektor

BSI-CC-PP-0098

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

Änderungsverlauf

Version	Datum	Änderungen
0.9.0	28.02.2017	Erstversion basierend auf BSI-CC-PP-0046, Version 1.2.8 vom 10.02.2016 mit den folgenden Anpassungen: Anpassungen eIDAS, Entfall xTV (gem. gematik Vorlage), Anpassungen wg. Spezifikationsänderungen, Entfall der optionalen Composite-Beziehung NK/AK, Entfall der Composite-Beziehung gSMC-K/AK, Entfall PP Konformität NK/AK, Übersetzung der CC SFR Texte DE → EN, Senkung des Angriffspotentials VAN.5 → VAN.3, allgemeine Fehlerbehebung, Anpassungen TLS NK, Anpassungen der Dokumentenstruktur, Aktualisierung des Literaturverzeichnisses, Abgleich Subjekte/ Objekte/ Attribute/ Operationen, Einarbeitung von Kommentaren
0.9.1	16.03.2017	• Erklärungen zu Abbildungen von O/OEs auf Bedrohungen, Annahmen und OSPs eingefügt (Abschnitt 4.5) • Erklärungen zur Abbildung von Sicherheitszielen auf SFRs eingefügt (Abschnitt 6.5)
0.9.2	17.03.2017	Bedrohungen, Annahmen, OSPs, Sicherheitsziele und SFRs aus dem PP-NK BSI-CC-PP-0097 eingefügt
1.0.0	18.04.2017	Version zur Abnahme durch gematik / BSI
1.0.1	28.07.2017	• Einarbeitung der Herstellerkommentare • aktuellere Alternativreferenzen zu [74] und [65] eingefügt • Anhang zu Informationsmodell eingefügt (Abschnitt 7.1) • Anhang zu CORS eingefügt
1.0.2	11.10.2017	• Editorielle Änderungen in Abschnitt 7.1 • Anpassung Anwendungshinweis bezüglich XSW Angriffen
1.0.3	13.11.2017	Einarbeitung der Kommentare der Prüfstelle
1.1	11.12.2017	Abgestimmte Version
1.2	08.05.2018	Anwendungshinweise zur Nutzung von AES-NI Fehlerkorrektur in FDP_IFF.1.2/NK.PF Anhang zu CORS entfernt
1.3	09.05.2018	Bereinigung Inkonsistenz zur Konnektor-Spezifikation bei TLS-Verbindungen zu Fachdiensten (Absatz 6.3.3.7)
1.4	03.07.2019	Einarbeitung Kommentare von Herstellern, Prüfstellen und BSI Bereinigung Inkonsistenz zur Konnektor-Spezifikation
1.5	27.01.2020	Anpassungen bzgl. TLS, RSAES-PKCS1-v1_5, nonQES XAdES, automatische Updates, Einarbeitung Kommentare des BSI
1.5.4	17.03.2020	Einarbeitung der Kommentare der Prüfstelle

Editorieller Hinweis:

Um die Konformität des Konnektors zum Schutzprofil BSI-CC-PP-0098 im Sinne einer sicheren Umsetzung der Sicherheitsanforderungen zu gewährleisten, wird dem Hersteller dringend empfohlen, seine Umsetzung der Sicherheitsfunktionalität frühzeitig mit der Zertifizierungsstelle abzustimmen. Hierdurch bekommt der Hersteller rechtzeitig ein Feedback, ob die getroffenen Maßnahmen zeitgemäß sind. Es wird explizit begrüßt, wenn bei dieser Abstimmung die mit der CC-Evaluierung beauftragte Prüfstelle mit dabei ist. Dem Hersteller muss aber bewusst sein, dass die Ergebnisse der Abstimmung nur unverbindlich sein können, da erst die CC-Evaluierung des Produkts nachweist, dass die konkrete Umsetzung der Sicherheitsfunktionalitäten gemäß gewählter AVA_VAN-Stufe sicher ist.

Inhaltsverzeichnis

1. PP-Einführung

1.1. PP-Referenz

Titel: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor

Version des Dokuments: 1.5.4

Datum des Dokuments: 17.03.2020

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

Registrierung: BSI-CC-PP-0098

Registrierung bei: Bundesamt für Sicherheit in der Informationstechnik (BSI)

CC Version: 3.1 (Revision 5)

Vertrauenswürdigkeitsstufe des Produktes: EAL3 erweitert um AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 und ALC_FLR.2

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

Editor: Initiale Erstellung sowie Pflege (BSI-CC-PP-0046 bis Version 1.2.8): Prüfstelle IT-Sicherheit der T-Systems GEI GmbH

Überarbeitung des Schutzprofils (zur BSI-CC-PP-00K+ Version 0.9.0): Holger Ebel (http://www.its-ebel.com)

Überarbeitung des Schutzprofils (zur BSI-CC-PP-0098 Version 1.1): SRC GmbH

Stichwörter: Gesundheitswesen, Telematikinfrastruktur, Konnektor, qualifizierte elektronische Signatur

Dieses Schutzprofil wurde erstellt auf der Grundlage folgender Dokumente:

[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

Darüber hinaus orientiert sich dieses Dokument in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang in Abschnitt 7.6 (insbesondere Abschnitt 7.6.5) aufgeführt sind; allen voran die Spezifikation Konnektor:

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

1.2. PP-Übersicht

Das Schutzprofil (PP) beschreibt und begründet die Sicherheitsanforderungen an den Konnektor gemäß Spezifikation [76]. Der Konnektor ist darauf ausgerichtet, durch Weiterentwicklung und Update im Feld für weitere Versionen nachgenutzt zu werden.

Der Konnektor besteht aus dem Netzkonnektor (NK) und dem Anwendungskonnektor (AK) und benötigt die Security Module Card Konnektor (gSMC-K).

Die Sicherheitsanforderungen an die Sicherheitsfunktionalität des Netzkonnektors sind, wenn dieser als Einzelkomponente evaluiert wird, im Schutzprofil BSI-CC-PP-0097 beschrieben.[1] Die Security Module Card Konnektor basiert auf einer Chipkarte mit einem Chipkartenbetriebssystem, das konform zum Schutzprofil BSI-CC-PP-0082 zertifiziert ist, und dem Objektsystem für gSMC-K, das nach TR-03144 zertifiziert ist. Es speichert Schlüsselmaterial für den Netzkonnektor und den Anwendungskonnektor 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 Schutzprofil BSI-CC-PP-0098 definiert die Sicherheitsanforderungen an den gesamten Konnektor.

Das Chipkartenbetriebssystem der gSMC-K ist konform zum Schutzprofil BSI-CC-PP-0082 [70] zertifiziert (A.AK.gSMC-K). Für die gSMC-K Chipkarte mit zertifiziertem Chipkartenbetriebssystem existiert eine eigene Spezifikation [80] und ein Schutzprofil [70].

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

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

[1] Werden Teile des Netzkonnektors evaluiert, sollte dem immer eine Evaluierung nach PP-0097 vorausgehen. Eine Evaluierung des Konnektors allein nach PP-0098 ist nach Common Criteria möglich jedoch nicht sinnvoll.

1.2.2. Terminologie

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

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

[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.

1.3. EVG-Beschreibung

Der Evaluierungsgegenstand (EVG) ist der Konnektor [76] für den Online-Rollout (Stufe 1).

Der EVG umfasst folgende Komponenten:

- den Netzkonnektor,
- den Anwendungskonnektor,
- das Fachmodul „Versichertenstammdatenmanagement“ (VSDM) [78].

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

1.3.1. EVG Typ

Der EVG ist ein Produkt bestehend aus o.g. Komponenten. 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. Das Fachmodul VSDM ändert den Produkttyp des EVG nicht.

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

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

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

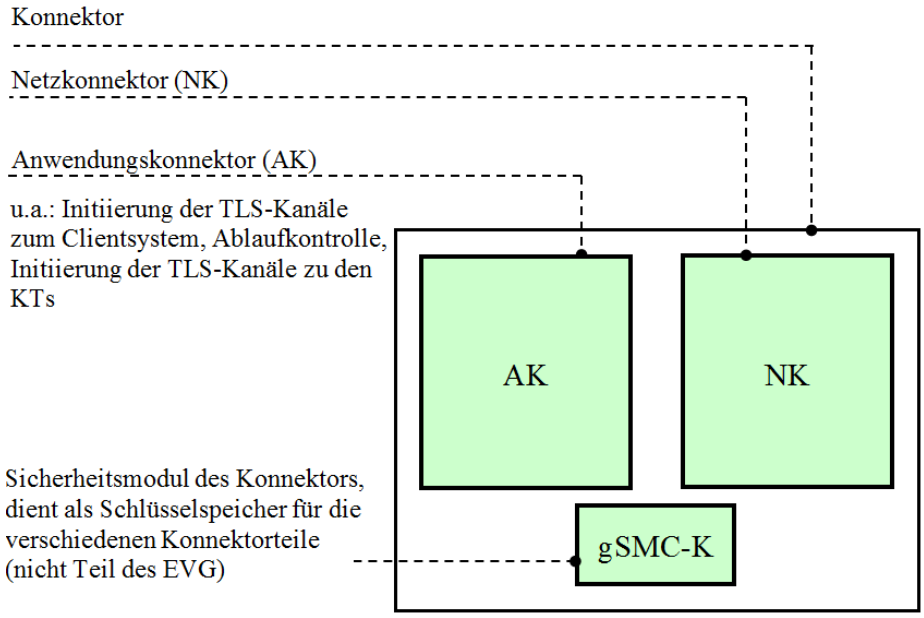


Abbildung 1: Funktionsblöcke des Konnektors

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[3] 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.

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

[3] Diese Authentisierung ist nicht Gegenstand des Schutzprofils.

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 [67]). Der Signaturdienst unterstützt darüber hinaus die Erstellung von qualifizierten Einfachsignaturen (s.a. [67]) 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 [76] zur Verfügung und erbringt Sicherheitsfunktionalität für deren sichere Nutzung und den Schutz der Ressourcen.

Der EVG kommuniziert mit den eHealth-Kartenterminals (eHKT, s. [77]) 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 [78].

Anwendungshinweis 1: Der Begriff VSDM Fachdienst umfasst im Rahmen dieses Schutzprofils 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 der 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 nach dem entsprechenden Schutzprofil evaluiert und zertifiziert wurde.

Es ist grundsätzlich nicht ausgeschlossen, Anwendungskonnektor und Netzkonnektor auf mehrere physische Einheiten zu verteilen bzw. als getrennte Produkte in jeweils eigenem Gehäuse zu gestalten und dennoch in Anlehnung an dieses Schutzprofil zu evaluieren. Hinweise dazu sind im Schutzprofil 1: Anforderungen an den Netzkonnektor [69] enthalten. Wenn nicht anders angegeben, wird in den folgenden Darstellungen stets von der Einbox-Lösung ausgegangen.

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

In Abbildung 2 bedeuten die Abkürzungen (siehe auch Kapitel 7.1):

- 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, Apotheken-verwaltungssystem, Krankenhaus-Informationssystem).
- PVS: Praxis-Verwaltungssystem. Dieser Ausdruck steht stellvertretend auch für Apotheken-Verwaltungssysteme (AVS) oder Krankenhaus-Informationssysteme (KIS). Er bezeichnet den Softwareanteil auf dem Clientsystem. Das Betriebssystem des Clientsystems ist in den folgenden Abbildungen nicht dargestellt.
- eGK: elektronische Gesundheitskarte

- HBA: Heilberufsausweis
- SM-B: Security Module Card Typ B oder HSM-B, Träger der kryptographischen Identität der Organisation
- gSMC-K: Sicherheitsmodul des Konnektors (nicht Teil des EVG)
- SIS: Sicherer Internet Service
- TI: Telematikinfrastruktur
- VSDM: Versichertenstammdatenmanagement
- VSDD: Versichertenstammdatendienst

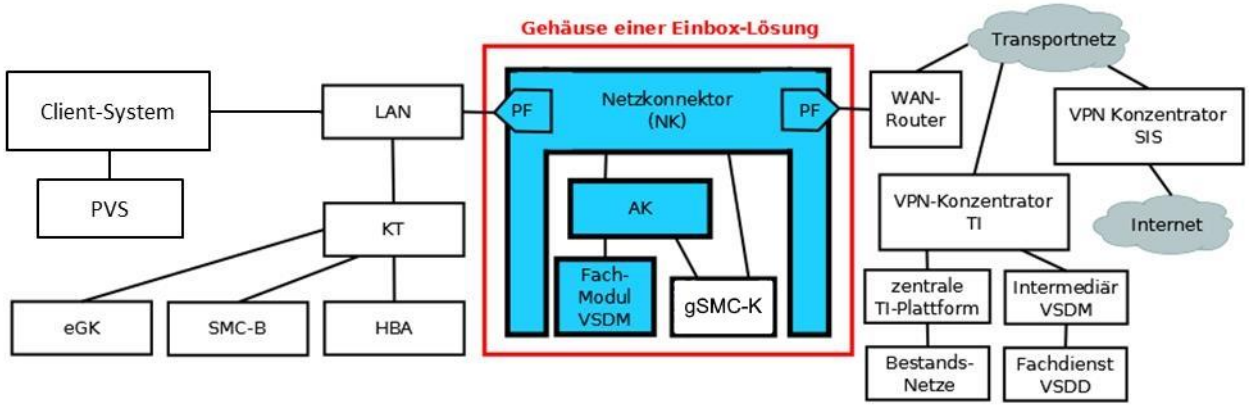


Abbildung 2: Einsatzumgebung des Konnektors (Einbox-Lösung)

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.

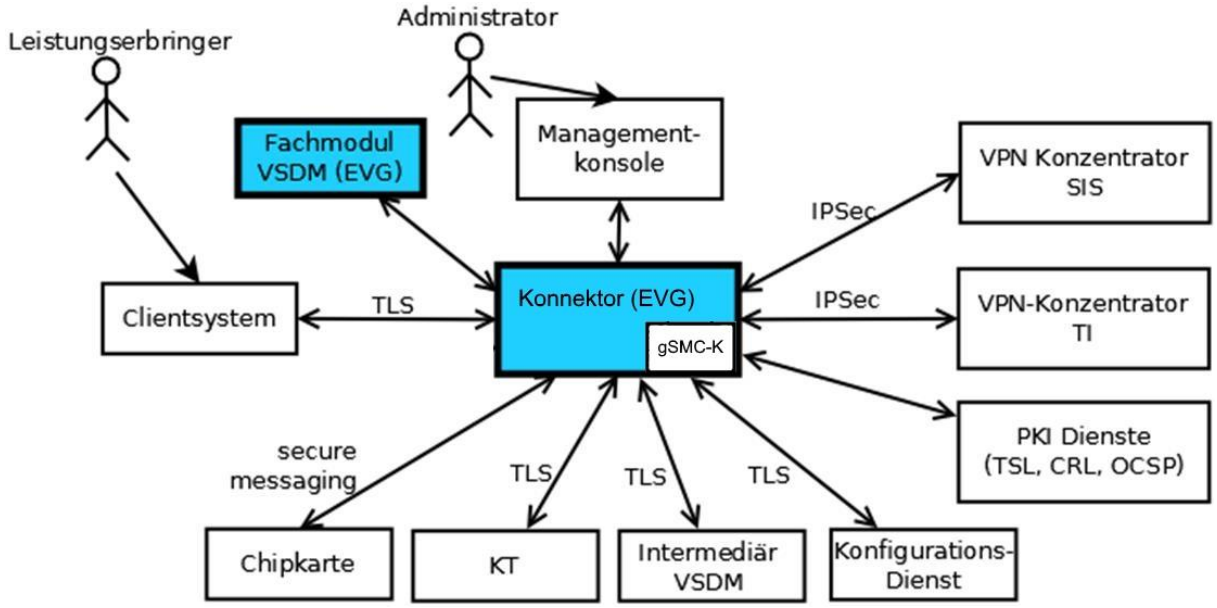


Abbildung 3: Logische Kanäle des EVG in seiner Einsatzumgebung

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, das konform zum Schutzprofil BSI-CC-PP-0082 zertifiziert ist, und dem Objektsystem für gSMC-K das nach TR-03144 zertifiziert ist. 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[4].

eHealth-Kartenterminals

Die eHealth-Kartenterminals sind gemäß Schutzprofil [71] evaluiert. Der EVG kommuniziert mit den eHealth-Kartenterminals über SICCT-Kommandos gemäß Spezifikation [77] [79] 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,

[4] 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 [76].

- 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,
- 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 [77], 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[5] 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. [67]), 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. [67]), 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.

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

Chipkarten

Der EVG identifiziert und authentisiert Chipkarten eGK, HBA und SMC-B vor ihrer Benutzung[6] und arbeitet nur mit Chipkarten zusammen, die gemäß den relevanten Schutzprofilen evaluiert und zertifiziert sind. Der EVG unterstützt darüber hinaus reduzierte 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[7] 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 [67]. 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 [69] (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 [69] (VPN-Client). Der damit verfügbare sichere Kanal verbindet das lokale

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

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

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**).

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.

1.3.3. Schnittstellen des Konnektors

1.3.3.1. Physische Schnittstellen des EVG

Anwendungshinweis 3: Der ST-Autor soll die Beschreibung der physischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Konnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern und zu begründen.

Der EVG besitzt folgende (externe) physische Schnittstellen (siehe auch Abbildung 2):

PS1 Eine Schnittstelle zum LAN bzw. zum Clientsystem.

Über diese Schnittstelle kann ein Clientsystem mit dem Anwendungskonnektor kommunizieren bzw. können ein Clientsystem oder andere Systeme im LAN mit dem Netzkonnektor 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 nicht notwendigerweise verschlüsselt sind.

Anwendungshinweis 4: Falls die mit PS1 bezeichnete LAN-Schnittstelle und die mit PS2 bezeichnete WAN-Schnittstelle in einer physischen Schnittstelle zusammenfallen, muss der ST-Autor nachweisen, dass der Konnektor trotzdem die Netze (LAN und WAN) sicher voneinander trennt.

PS3 Eine Schnittstelle zum Sicherheitsmodul gSMC-K.

Das Sicherheitsmodul gSMC-K stellt Sicherheitsfunktionalität zur Speicherung von Schlüsselmaterial und kryptographische Sicherheitsfunktionen für den Netzkonnektor und den Anwendungskonnektor bereit.

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

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.

Anwendungshinweis 5: Der ST-Autor soll die Schnittstellen nach Möglichkeit in Form einer Skizze grafisch darstellen. Dazu kann auch auf die bereits in Abschnitt 1.3.2 enthaltene Abbildung verwiesen werden.

1.3.3.2. Logische Schnittstellen des EVG

Anwendungshinweis 6: Der ST-Autor soll die Beschreibung der logischen Schnittstellen abhängig von der konkreten Ausgestaltung des Produkts anpassen. Es wird erwartet, dass ein Konnektor über die im Folgenden aufgelisteten Schnittstellen verfügt. Sofern der ST-Autor davon abweicht, sind die Abweichungen zu erläutern.

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

LS1 (gelöscht)

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

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

LS4 Eine Schnittstelle zum VPN Konzentrator der zentralen TI-Plattform (WAN, via PS2[8]).

LS5 Eine Schnittstelle zum VPN Konzentrator des sicheren Zugangspunkt des Internet-Providers (SIS) (WAN, via PS2[9]).

LS6 Eine Schnittstelle zu Fachdiensten, die mittels eines VPN über das Transportnetz (WAN, via PS2[10]) erreicht werden.

[8] In der Konnektorspezifikation [76] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[9] In der Konnektorspezifikation [76] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

LS7 Eine Schnittstelle zu PKI- und anderen Diensten (WAN, via PS2[11]). Dazu zählen der TSL-Dienst, der CRL-Download, sowie OCSP-Dienst.

LS8 Eine Schnittstelle zum Konfigurationsdienst (WAN, via PS2[12]).

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 Eine Schnittstelle zu möglicherweise proprietären (herstellerspezifischen) Managementfunktionen des Konnektors (via PS1 und PS2, siehe Kapitel 4.3 in [76]).

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

1.3.4. Aufbau und physische Abgrenzung des Konnektors

Zur Gesamtarchitektur und für einen Überblick über die Kernkonzepte sei auf die Architektur der TI-Plattform [73] in ihrer jeweils aktuellen Version verwiesen. Eine grobe Abgrenzung des Konnektors von den übrigen Teilen des Konnektors erfolgte bereits in Abschnitt 1.3.

Anwendungshinweis 7: Der ST-Autor soll in diesem Abschnitt die Architektur seines Produkts beschreiben. Dabei soll er sich an der aktuellen Version der Spezifikation Konnektor [76] orientieren. Siehe auch die Hinweise in Abschnitt 7.6.4 und 7.6.5 in [69].

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. Vom Netzkonnektor erbrachte Sicherheitsdienste

Der EVG-Teil Netzkonnektor erbringt seine Sicherheitsdienste über die in der Konnektor-Spezifikation [76] definierten Schnittstellen weitgehend automatisch. Der Netzkonnektor ermöglicht ein Management (Administration) seiner Funktionalitäten nach Autorisierung des Administrators im Konnektor. Die Authentisierung des Administrators kann durch den Anwendungskonnektor erfolgen.

---

[10] In der Konnektorspezifikation [76] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

[11] In der Konnektorspezifikation [76] 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 [76] sind Szenarien definiert, die für eine Verbindung zum WAN ebenfalls die Schnittstelle PS1 vorsehen. In diesen Fällen bleibt die Schnittstelle PS2 ungenutzt.

Anwendungshinweis 8: **Authentisierung des Administrators:** Im Fall einer Einbox-Lösung, die in diesem Schutzprofil angenommen wird, erscheint ein gemeinsamer Administrator-Account für mehrere Konnektorteile wünschenswert. Daher erlaubt dieses Schutzprofil, dass die Authentisierung des Konnektor-Administrators vom NK oder vom AK vorgenommen werden kann. Der jeweils andere Konnektorteil (AK oder NK) kann den Authentisierungszustand übernehmen und auf diese Weise die Zugriffe des Administrators autorisieren. Aufgrund der Annahme A.AK.phys_Schutz ist dabei keine zusätzliche Authentisierung zwischen den Konnektorteilen (NK und AK) erforderlich. In diesem Schutzprofil wird davon ausgegangen, dass die Authentisierung des Konnektor-Administrators vom AK vorgenommen wird. Das Umgebungsziel OE.NK.Admin_Auth des Netzkonnektors wird daher durch das EVG-Ziel O.AK.Admin des Anwendungskonnektors direkt erfüllt. Das Schutzprofil verbietet nicht, dass der Netzkonnektor die Authentisierung des Administrators auch selbst durchführen kann; in diesem Fall ist das Umgebungsziel OE.NK.Admin_Auth in ein EVG-Ziel umzuwandeln.

Anwendungshinweis 9: **Vollständigkeit der Dienste:** Die Liste der im Folgenden genannten Dienste ist in dem Sinne vollständig, dass man sich weitere Dienste zwar vorstellen könnte, solche Dienste aber im Schutzprofil BSI-CC-PP-0097 [69] bewusst nicht modelliert wurden.

- Beispielsweise erzwingt der VPN-Konzentrator die Nutzung des VPN-Tunnels (er leitet nur Pakete aus dem VPN-Tunnel zu den Fachdiensten weiter). Der Netzkonnektor **unterstützt den VPN-Konzentrator** dabei, indem er das andere Ende des VPN-Tunnels implementiert. Dies stellt aber keine gesonderte Sicherheitsfunktionalität dar, sondern wird bereits unter Sicherheitsdienst VPN-Client beschrieben.
- Eine **Vorabprüfung der Datensätze auf Plausibilität** (z. B. XML-Validierung) wird durch den Anwendungskonnektor vorgenommen; dies stellt für den Netzkonnektor keine Sicherheitsfunktionalität dar.
- Eine hohe **Verfügbarkeit des Konnektors** ist natürlich ein wichtiges Ziel im Gesundheitswesen. Bei Nutzung von Infrastrukturen wie z. B. dem Internet kann eine bestimmte Verfügbarkeit jedoch nicht garantiert werden, weil diese von vielen nicht beeinflussbaren Einzelheiten abhängig ist. Daher wurde in diesem Schutzprofil darauf verzichtet, die Verfügbarkeit als Sicherheitsziel (siehe Abschnitt 4.1) zu formalisieren. Gleiches gilt sinngemäß für Quality of Service. Siehe auch [69], Abschnitt 7.6.8. Anforderungen an die Verfügbarkeit von Konnektoren werden im Rahmen des Zulassungsverfahrens für die Konnektoren berücksichtigt.

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

Der Netzkonnektor erbringt folgende Sicherheitsdienste:

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.

a) 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.

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

Der Netzkonnektor muss die Benutzung des VPN-Tunnels für den Versand von Daten zur zentralen Telematikinfrastruktur-Plattform und den darüber zugänglichen Netzen erzwingen und ungeschützten Zugriff auf das Transportnetz verbieten. Der Konnektor kann nicht verhindern, dass ein Leistungserbringer zu schützende Daten der TI und der Bestandsnetze absichtlich preisgibt[13], 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 wehrt der Netzkonnektor wegen der Augmentierung mit AVA_VAN.5 in BSI-CC-PP-0097 [69] Angriffe mit hohem Angriffspotential ab. Der Netzkonnektor beschränkt den freien Zugang zu dem und von dem als unsicher angesehenen Transportnetz. Die Inhalte der Kommunikation zur Telematikinfrastruktur werden vom 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[14] sowie Verbindungen zum CRL Download Server.

Anwendungshinweis 11: Bei der Betrachtung von Angriffen aus dem LAN sind auch solche Bedrohungsszenarien zu berücksichtigen, bei denen auf anderen Wegen (z. B. Wechseldatenträger wie CD, DVD, USB-Stick, Diskette) Schadsoftware in die IT-Systeme im LAN des Leistungserbringers kommen kann. Ein **LAN-seitiger Paketfilter** hindert solche Schadsoftware daran, die Integrität des Konnektors zu bedrohen.

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

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

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

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: Hinweis: Die Entscheidung, für welche Verbindungen diese TLS-Kanäle genutzt werden, liegt beim Anwendungskonnektor. Der Verfasser eines konformen STs kann aber auch solche Aspekte ganz oder teilweise dem Netzkonnektor zuordnen.

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 genutzt, um die Audit-Daten des Sicherheits-Logs mit einem Zeitstempel zu versehen.

Anwendungshinweis 14: Der ST-Autor kann optional Maßnahmen zur **Sicherung des Kommunikationskanals** zwischen dem Netzkonnektor und dem zentralen Zeitdienst fordern, sofern dies von der zentralen Infrastruktur unterstützt wird. Als Maßnahmen kommen insbesondere in Frage: (a) Integritätsschutz der übertragenen Zeit und (b) vorherige Authentisierung des zentralen Zeitdienstes gegenüber dem Netzkonnektor. Mindestens gefordert ist eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeit (maximale Abweichung), siehe FPT_STM.1/NK. Zu beachten ist, dass die Konnektor-Spezifikation [76] vorsieht, dass die Zeitsynchronisation ausschließlich mit Servern innerhalb der zentralen Telematikinfrastruktur-Plattform erfolgt, d.h. über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur. Der ST-Autor soll beschreiben, welche Funktionalität genau der Netzkonnektor bietet. Die Funktionalität soll sich dabei an den aktuellen Versionen der Konnektor-Spezifikation [76] orientieren.

DHCP-Dienst: Der Netzkonnektor stellt an der LAN-Schnittstelle (PS1) die Funktion eines DHCP Servers gemäß RFC 2131 [45] und RFC 2132 [46] zur Verfügung.

DNS-Dienst: Der Netzkonnektor stellt an der LAN-Schnittstelle (PS1) und an der Schnittstelle zum AK die Funktion eines DNS-Servers zur Verfügung. Über die Schnittstelle LS3 stellt der AK diese Funktion auch den Fachmodulen bereit.

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.[15] 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) bereitgestellt, die der Netzkonnektor ebenfalls auswertet. Außerdem überprüft der Netzkonnektor, dass die verwendeten Algorithmen gültig sind. Siehe auch Sicherheitsdienst VPN-Client (a): Authentisierung der Kommunikationspartner).

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

Anwendungshinweis 15: Die Prüfung der Algorithmen kann implizit durch den Netzkonnektor erfolgen, indem sichergestellt wird (z. B. im Rahmen der Evaluierung), dass der Netzkonnektor nur gültige Algorithmen verwendet. Es ist im Sinne des Schutzprofils zulässig, wenn die Verwendung ungültig gewordener Algorithmen dadurch verhindert wird, dass der Netzkonnektor entsprechend konfiguriert wird oder dass – unter Verwendung des Software-Update-Mechanismus des EVG bzw. des Gesamtkonnektors – 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 soll kein netzwerkbasiertes Intrusion Detection System (IDS) für das Clientsystemnetz realisieren.

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 EVGs 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 [76].

Anwendungshinweis 17: Die Auswertung des Sicherheits-Logs kann sowohl durch den Netzkonnektor als auch durch die Einsatzumgebung erfolgen. Der ST-Autor soll beschreiben, welche Funktionalität genau der Netzkonnektor bietet.

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

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

Anwendungshinweis 19: Es soll möglich sein, Wartungsaktivitäten (einschließlich Monitoring und Konfiguration) durchzuführen, ohne den zertifizierten Status des Netzkonnektors zu verlieren (dabei wird davon ausgegangen, dass bei der Wartung die Benutzer- und Administratordokumentation des Netzkonnektors beachtet wird). Abhängig von der Mächtigkeit der Wartungsschnittstelle sind spezifische Separationsmechanismen erforderlich, welche sicherstellen, dass die Sicherheitsfunktionalitäten des Netzkonnektors durch die Wartung nicht beeinträchtigt werden. Der ST-Autor kann auch eine Verfeinerung der Komponenten AGD_OPE.1 in Betracht ziehen.

> Die Schnittstellen zum lokalen Management des Konnektors sind herstellerspezifisch. Der Umfang der möglichen Wartungsaktivitäten kann unterschiedlich sein. Der ST-Autor soll beschreiben, welche Funktionalität genau der Netzkonnektor bietet.
>
> Eine Möglichkeit zur Fernwartung ist wünschenswert, wird aber in diesem Schutzprofil nicht verpflichtend gefordert (wohl aber in der Konnektor-Spezifikation [76], Abschnitt 4.3). Falls eine Möglichkeit zur Fernwartung vorhanden ist, muss diese hinreichend gut abgesichert werden. Zur Absicherung der Fernwartung können dieselben oder ähnliche Mechanismen verwendet werden wie zur Absicherung der lokalen Administration an der LAN-Schnittstelle (z. B. sicherer TLS-Kanal zwischen Administrator-Arbeitsplatz und Netzkonnektor wie bei FTP_TRP.1/NK.Admin, Autorisierung des Administrators wie bei FMT_MSA.4/NK). Es ist jedoch zu beachten, dass laut Konnektorspezifikation (Kapitel 4.3.8) bei einer Managementverbindung über die WAN Schnittstelle der Verbindungsaufbau immer vom Konnektor ausgehen muss.

Der Netzkonnektor erzwingt eine sichere **Authentisierung des Administrators** vor administrativen Aktivitäten. Die Authentisierung selbst kann dabei durch den Netzkonnektor oder durch den Anwendungskonnektor übernommen werden, s. Anwendungshinweis 8. Die Zugriffskontrolle für die Administration des Netzkonnektors (nur authentisierte Administratoren dürfen administrative Tätigkeiten und Wartungsarbeiten durchführen) ist Sicherheitsfunktionalität des Netzkonnektors.

1.3.5.2. Vom Anwendungskonnektor erbrachte Sicherheitsdienste

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

Signaturdienst: Der EVG ermöglicht im Sinne der eIDAS-VO [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 möglich. Als qualifizierte Signaturerstellungseinheit (QSEE) kommt für QES ein Heilberufsausweis (HBAx[16]) mit QES-Signaturschlüsseln zum Einsatz. Für die Erzeugung der nonQES-Signatur wird ein HBAx oder die SM-B[17] 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,
- Signaturattribute: einfache Dokumentensignatur, Parallelsignatur, Gegensignatur.

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

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

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 Signatur.
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 [76] werden folgende Dokumenten-Formate zur Signaturerstellung und Signaturprüfung unterstützt[18]:

- 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. [76], Kap. 4.1.8):

- Adobe-Standard (für PDF/A-Dokumente): PAdES
- CMS (RFC 5652, [33]): CAdES
- XMLDSig (für XML-Dokumente): XAdES
- S/MIME [34]
- 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 [76] festgelegt.

Der folgende Abschnitt enthält einen beispielhaften Ablauf einer qualifizierten Signatur-Erzeugung im Fall der fehlerfreien Ausführung.

Für die qualifizierte und nicht-qualifizierte elektronische Signatur werden die zu signierenden bzw. zu prüfenden Dokumente vom Client-System an der Außenschnittstelle des Konnektors übergeben. Eine eventuelle Anzeige der Dokumente und ggf. Auswahl, welche Dokumente eines Stapels signiert werden sollen und welche nicht, findet vorgelagert außerhalb des EVG auf dem Clientsystem statt. Die zu signierenden bzw. zu prüfenden Dokumente werden bei der Übermittlung entsprechend den Darstellungen in Absatz 1.3.2 und Abbildung 2 geschützt.

Um dem Benutzer bei der PIN-Eingabe für einen Signaturauftrag eine eindeutige Identifizierung des Auftrags zu ermöglichen, ist für jeden Signaturauftrag eine Jobnummer

[18] Die entsprechenden Standards sind der Konnektor-Spezifikation zu entnehmen, siehe Tabelle 148 in [76]

notwendig. Ein Clientsystem muss daher eine Jobnummer mit jedem Signaturauftrag an den EVG übersenden.

Der EVG stellt diese Jobnummer über eine Schnittstelle dem Clientsystem zur Verfügung. Die Kommunikation zwischen Clientsystem und EVG (s. auch Abbildung 2) ist dabei wie im Sicherheitsdienst "Gesicherte Kommunikation" des Anwendungskonnektors beschrieben geschützt.

Bei einer vorgelagerten Anzeige der zu signierenden Dokumente muss das Clientsystem die Jobnummer anzeigen. Zur Identifizierung des Signaturauftrags durch den Nutzer wird die Jobnummer vom EVG an das eHealth-Kartenterminal gesendet und dort bei der PIN-Eingabe im Display angezeigt.

Der EVG stellt dem Clientsystem zusätzlich den Fortschritt einer Stapelsignatur (Ereignismeldung nach jeder erfolgreichen Signatur eines Dokuments des Stapels) über den Systeminformationsdienst zur Verfügung. Ebenso ist der Abbruch einer Stapelsignatur durch den Nutzer über das Clientsystem möglich, wobei Signaturen eines bereits finalisierten Teilstapels erhalten bleiben jedoch erstellte Signaturen eines aktuell bearbeiteten und noch nicht finalisierten Teilstapels verworfen werden.

Die dargestellte Erzeugung einer QES erfolgt in folgenden Schritten:

1. Der EVG bekommt einen Auftrag, für einen identifizierten Signierenden und die übergebenen Dokumente eine QES zu erzeugen, dabei kann es sich um einen Stapel- oder Einzelsignaturauftrag handeln.
2. Für den Signierenden wird das Kartenterminal mit der gesteckten Signaturkarte (dem HBA des Signierenden) ermittelt.
3. Es werden die auf der Signaturkarte verfügbaren Signatur-Zertifikate und ggf. Attributzertifikate ermittelt und geprüft.
4. Im übergebenen Dokument werden die zu signierenden Daten identifiziert (DTBS) und deren Digest berechnet. Im Fall von XML-Signaturen wird die Wohlgeformtheit und die Validität gegen das XML-Schema des Dokumentes und die Auswahl der zu signierenden Daten geprüft.
5. Im Fall einer Stapelsignatur wird ein gesicherter Kanal zwischen der gSMC-K und der Signaturkarte aufgebaut.
6. Am Kartenterminal des Benutzers wird die PIN-Abfrage zur Autorisierung der Signatur mit der QSEE (HBA) durchgeführt. Dazu dient die gesteckte gSMC-KT als Remote-PIN-Sender. Am Display des Kartenterminals wird die vom Clientsystem übergebene Jobnummer angezeigt, die den aktuellen Signaturvorgang eindeutig identifiziert.
7. Es erfolgt die Auslösung des Signaturvorgangs durch Eingabe der Signatur-PIN am eHealth-Kartenterminal mit der angezeigten Jobnummer des Signaturauftrages.
8. Die Signaturen über die Digests der zu signierenden Dokumente werden in der QSEE generiert und zum EVG übertragen.
9. Der EVG prüft die Korrektheit der erzeugten digitalen Signatur unter Verwendung des Digest, des Wertes der Signatur und des Zertifikates der QSEE für jede empfangene digitale Signatur und im Fall der Stapelsignatur die Menge der empfangenen Signaturen gegen die Liste der zu signierenden Dokumente. Bei Abweichungen wird

die Signaturerzeugung für die Dokumente des Stapels abgebrochen und alle bisher erzeugten Signaturen werden verworfen und sicher vom EVG gelöscht.

10. Der EVG erzeugt für ordnungsgemäß erzeugte Signaturen die resultierenden, signierten Dokumente entsprechend dem gewünschten Format.
11. Die signierten Dokumente werden an das Clientsystem ausgegeben.

Anwendungshinweis 20: Die genauen Abläufe sind der Spezifikation Konnektor [76] und den dort referenzierten Dokumenten zu entnehmen.

Für die Erzeugung von nichtqualifizierten elektronischen Signaturen ist der prinzipielle Ablauf eine Teilmenge der o.g. Abläufe. Insofern ergeben sich dafür keine zusätzlichen Sicherheitseigenschaften.

Der folgende Abschnitt enthält einen beispielhaften Ablauf einer qualifizierten Signatur-Prüfung im Fall der fehlerfreien Ausführung.

1. Der EVG erhält einen Auftrag zur Verifizierung eines signierten Dokumentes mit einer QES.
2. Das übergebene Dokument wird auf Konformität gegen die entsprechenden Dokumentenstandards und Signaturformate validiert.
3. Jede dem Dokument zugeordnete digitale Signatur wird durch Schritt 4 geprüft und das Ergebnis im Schritt 5 ausgegeben.
4. Die zur Verifizierung benötigte Zertifikatskette bzw. Zertifikatsketten (Signaturzertifikat und CA-Zertifikat) werden aufgebaut (das zum Signaturzertifikat gehörende CA-Zertifikat wird der BNetzA-VL entnommen) und deren Signaturen und die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt überprüft und das Ergebnis im Schritt 5 ausgegeben. Der anzunehmende Signaturerstellungszeitpunkt ist aus den zur Signaturprüfung vorliegenden Informationen abzuleiten. Dem Verifizierenden muss ermöglicht werden, selbst einen angenommenen Signaturerstellungszeitpunkt anzugeben, zu dem die Signatur geprüft werden soll.
5. Die Verifikationsergebnisse werden an das Clientsystem ausgegeben

Anwendungshinweis 21: Weitere Informationen zu den Abläufen sind der Spezifikation Konnektor [76] und den dort referenzierten Dokumenten zu entnehmen.

Für die Verifizierung von nichtqualifizierten elektronischen Signaturen ist der Ablauf identisch.

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 [76] 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 [68] 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, [33]) 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, [34]).

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[19]. Der Zugriff von Clientsystemen ist durch die Verwendung von Whitelisting einschränkbar;
- Verbindungen zwischen dem EVG und Fachdiensten bzw. deren vorgelagerten Intermediären;

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

- Verbindungen zwischen dem EVG und eHealth-Kartenterminals;
- Verbindungen zwischen dem EVG und einem externen Managementsystem;
- Verbindungen zwischen dem EVG und dem Konfigurationsdienst.
- Verbindungen zwischen dem EVG und dem TSL-Dienst für den Download der BNetzA-VL und deren Hash-Wert.

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

TLS Dienst: 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[20]. Beim Aufbau dieser TLS-Kanäle wird die Authentizität der Endpunkte durch Verwendung von Zertifikaten überprüft. Bei der Authentisierung gegenüber Fachdiensten kann der Konnektor die Identität einer SMC-B über einen entsprechenden Kanal nutzen. Bei fehlerhafter Authentisierung wird die Verbindung bzw. der Verbindungsaufbau abgebrochen.

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

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

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

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

[20] Siehe auch Sicherheitsdienst „gesicherte Kommunikation“

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 [67]. 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 [76], 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 EVG immer mit dem Konnektorteil Security Module Card Konnektor gSMC-K gemeinsam betrieben, siehe auch die Beschreibung zur Einsatzumgebung in Kapitel 1.3.2.

Der EVG nutzt die Sicherheitsfunktion der gSMC-K. Das Betriebsystem der gSMC-K muss nach dem Schutzprofil *Card Operating System (PP COS)* [70] evaluiert und zertifiziert sein. Das Objektsystem der gSMC-K muss nach der Technischen Richtlinie TR-03144 [72] evaluiert und zertifiziert sein.

Anwendungshinweis 22: Der Konnektor kann sowohl als reine Software-Lösung implementiert werden als auch in Form einer aus Hardware und Software bestehenden Box, siehe auch [69], Abschnitt 7.6.4. Wenn die Hardware nicht Teil des EVGs ist, soll der Verfasser des STs in diesem Kapitel exakte Angaben zur zugrundeliegenden Hardware machen, insbesondere wenn die Hardware zum sicheren Betrieb des EVGs beiträgt (z.B beim sicheren Start des Netzkonnektors). Im Rahmen von ADV_ARC müssen entsprechende Nachweise erbracht werden, dass die Sicherheit des EVGs (unter Berücksichtigung der Einsatzumgebung) durch die Hardware nicht beeinträchtigt wird. Es soll dabei gezeigt werden, dass die Annahme einer sicheren Hardware gerechtfertigt ist. Insbesondere sind kritische Hardware-Komponenten wie zum Beispiel Netzwerkcontroller oder für den sicheren Start relevante Komponenten zu betrachten.

2. Postulat der Übereinstimmung

2.1. Common Criteria Konformität

Das Schutzprofil wurde gemäß Common Criteria, Version 3.1, Revision 5, erstellt und ist

CC Teil 2 [2] erweitert (extended) und

CC Teil 3 [3] konform (conformant).

2.2. Schutzprofil-Konformität

Dieses Schutzprofil behauptet keine Konformität zu einem anderen Schutzprofil.

2.3. Paket-Konformität

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, erweitert um die 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).

2.4. Begründung der Konformität

Es wurden die in Kapitel 5 beschriebenen, über CC Teil 2 [2] hinausgehenden funktionalen Anforderungen und keine über CC Teil 3 [3] hinausgehenden Anforderungen an die Vertrauenswürdigkeit definiert.

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

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, wie sie in CC Teil 3 [3] definiert ist, zusammen mit der Komponente AVA_VAN.3, um Schutz gegen „Enhanced-Basic“ Angriffspotenzial zu erreichen.

Durch direkte 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 Kapitel 6.5. Die Erweiterung und das Augmentieren von Komponenten ist zulässig.

2.5. Festlegung der Konformität

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

strict conformance

behaupten.

2.6. PP-Organisation

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

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 Sicherheitsziele.

3.1.1. Zu schützende Werte

3.1.1.1. Durch den Netzkonnektor zu schützende Werte

Die folgenden zu schützenden Werte sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen[21]:

Die primären Werte sind in der folgenden Tabelle 1 aufgeführt.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur-Plattform (beide Übertragungsrichtungen)	Vertraulichkeit, Integrität, Authentizität	Zwischen den lokalen Netzen der Leistungserbringer und der zentralen Telematikinfrastruktur-Plattform werden zu schützende Daten der TI und der Bestandsnetze ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der Absender von übertragenen Daten muss eindeutig bestimmbar sein. ⇒ T.NK.local_EVG_LAN, T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_VPN_Data, A.NK.AK, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.Zert_Prüf, T.NK.DNS

[21] Der Begriff „zu schützende Daten der TI“ wird in [69] wie folgt definiert: *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.*

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Nutzerdaten während der Übertragung zwischen Konnektor und sicherem Internet Service	Vertraulichkeit, Integrität, Authentizität	Beim Zugriff auf Internet-Dienste werden Nutzerdaten zwischen den lokalen Netzen der Leistungserbringer und dem sicheren Zugangspunkt zum Internet ausgetauscht. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Der angegebene Schutz der Authentizität bezieht sich auf die Tunnel-Endpunkte, nicht auf die im Tunnel übertragenen Daten. ⇒ T.NK.local_EVG_LAN, T.NK.remote_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_VPN_Data, A.NK.AK, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.DNS
zu schützende Daten der TI und der Bestandsnetze im Clientsystem	Vertraulichkeit, Integrität	Auf den Clientsystemen werden zu schützende Daten der TI und der Bestandsnetze vorgehalten. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten manipulieren können. ⇒ T.NK.remote_EVG_LAN, A.NK.phys_Schutz
in der zentralen Telematikinfrastruk-tur-Plattform gespeicherte zu schützende Daten der TI und der Bestandsnetze	Vertraulichkeit, Integrität	Werden zu schützende Daten der TI und der Bestandsnetze in der zentralen Telematik-infrastruktur-Plattform gespeichert, so dürfen diese, abhängig von ihrem Schutzbedarf (abhängig vom Fachdienst), auch dort nicht unbefugt eingesehen oder unbemerkt verändert werden können. ⇒ T.NK.remote_VPN_Data, A.NK.sichere_TI
Clientsystem, Anwendungs-konnektor	Integrität	Manipulierte Clientsysteme oder Anwendungs-konnektoren können dazu führen, dass zu schützende Daten der TI und der Bestandsnetze abfließen oder unautorisiert verändert werden. Im normalen Betrieb wird davon ausgegangen, dass zu schützende Daten der TI und der Bestandsnetze das Clientsystem nur dann verlassen, wenn sie in die zentrale Telematikinfrastruktur-Plattform oder auf eine eGK übertragen werden sollen. Daher werden zu schützende Daten der TI und der Bestandsnetze nur durch den Anwendungskonnektor bzw. (im Fall von Daten der Bestandsnetze) den Netzkonnektor übermittelt. Ein manipuliertes Clientsystem könnte

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

Tabelle 1: Primäre Werte des Netzkonnektors

Die sekundären Werte sind in der folgenden Tabelle 2 aufgeführt:

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
zu schützende Daten der TI und der Bestandsnetze im Netzkonnektor	Vertraulichkeit, Integrität	Auch während der Verarbeitung im Netzkonnektor 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	Vertraulichkeit,	Gelingt es einem Angreifer, Kenntnis von

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
Schlüsselmaterial (während seiner Speicherung im Netzkonnektor oder Verwendung durch den Netzkonnektor)	Integrität, Authentizität	Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der Netzkonnektor seine Sicherheitsleistungen korrekt erbringt. Werden Sitzungsschlüssel ausgetauscht, so ist vorher die Authentizität des Kommunikationspartners sicherzustellen. ⇒ A.NK.phys_Schutz, T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit, T.NK.Zert_Prüf
Authentisierungs-geheimnisse (im Netzkonnektor gespeicherte Referenzdaten und zum Netzkonnektor übertragene Verifikationsdaten)	Vertraulichkeit	Die Vertraulichkeit von Authentisierungs-geheimnissen (z. B. Passwort für Administrator-authentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit)
Management-Daten (während ihrer Übertragung zum Netzkonnektor)	Vertraulichkeit, Integrität und Authentizität	Wenn der Netzkonnektor 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 Netzkonnektor)	Integrität	Management-Daten (z. B. Konfigurationsdaten) des Netzkonnektors dürfen nicht unbemerkt verändert werden können, da sonst nicht mehr sichergestellt ist, dass der Netzkonnektor seine Sicherheitsleistungen korrekt erbringt. ⇒ A.NK.phys_Schutz, alle Bedrohungen, gegen die O.NK.Schutz wirkt (T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit)
Sicherheits-Log-Daten (Audit-Daten)	Integrität, Verfügbarkeit	Der Netzkonnektor muss Sicherheits-Log-Daten generieren, anhand derer Veränderungen an der Konfiguration des Netzkonnektors nachvollzogen werden können (vgl. O.NK.Protokoll und

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen bzw. erforderliche Annahmen
		FAU_GEN.1/NK.SecLog). Niemand darf Sicherheits-Log-Daten löschen oder verändern können. Wenn der für die Sicherheits-Log-Daten vorgesehene Speicherbereich aufgebraucht ist, können die Sicherheits-Log-Daten zyklisch überschrieben werden. Die Sicherheits-Log-Daten müssen auch zum Nachweis der Aktivitäten von Administratoren verwendet werden können. ⇒ T.NK.local_EVG_LAN, T.NK.remote_EVG_WAN, T.NK.remote_EVG_LAN, T.NK.local_admin_LAN, T.NK.remote_admin_WAN, T.NK.counterfeit
Systemzeit	Verfügbarkeit, Gültigkeit	Der Netzkonnektor muss eine gültige Systemzeit vorhalten und diese regelmäßig mit Zeitservern synchronisieren. Die Zeit wird für die Prüfung der Gültigkeit von VPN-Zertifikaten sowie für die Erzeugung von Zeitstempeln in Sicherheits-Log-Daten oder Audit-Daten verwendet. ⇒ T.NK.TimeSync

Tabelle 2: Sekundäre Werte des Netzkonnektors

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 3 zusammengestellt sind. Der Begriff „zu schützende Daten der TI“ aus dem Schutzprofil BSI-CC-PP-0097 [69] wird hier in folgender Weise erweitert: in [69] wird der Begriff definiert als „*medizinische oder sonstige personenbezogene Daten (einschließlich Daten des Versicherten), die aus dem Zuständigkeitsbereich des Leistungserbringers in die Verantwortung der Telematikinfrastruktur übergehen*“. In diesem Schutzprofil wird der Begriff ***Nutzerdaten*** verwendet, der den Begriff „zu schützende Daten der TI“ enthält und erweitert um sonstige Daten, die auf Anforderung des Benutzers vom EVG bearbeitet, gespeichert oder übertragen werden. Dazu gehören beispielsweise beliebige Dokumente, die durch den EVG signiert werden sollen oder deren Signatur überprüft werden soll. Weiterhin wird der Begriff ***Metadaten*** für Daten verwendet, die im Sinne von Steuer- oder Ergebnisdaten im Zusammenhang mit der Verarbeitung, Speicherung oder Übertragung von Nutzerdaten auftreten. Hierzu zählen beispielsweise Parametersätze beim Aufruf von Funktionalitäten des EVG durch Clientsysteme oder Ergebnisse von solchen Aufrufen. Hinzu kommen noch ***TSF-Daten***, die zur Umsetzung der Sicherheitsfunktionen des EVG notwendig sind [1].

Bei den zu schützenden Werten wird zwischen primären und sekundären Werten unterschieden, deren Definition aus [69] übernommen wurde:

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

Die zu schützenden Werte sind in den folgenden Tabellen Tabelle 3 und Tabelle 4 aufgeführt.

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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
		⇒ 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.[22] ⇒ T.AK.Mani.EVG, T.AK.Mani.TI, A.AK.Konnektor, A.AK.phys_Schutz

Tabelle 3: primäre Werte des Anwendungskonnektors

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 Authentisierungsgeheimnisse 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, Authentisierungsgeheimnisse, kryptografische	Integrität, Vertraulichkeit	Die Daten, Authentisierungsgeheimnisse und kryptografische Daten während der Bearbeitung und Speicherung innerhalb der externen Chipkarte dürfen

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

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

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
		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 4: sekundäre Werte des Anwendungskonnektors

Der für die Signaturerstellung notwendige Signaturschlüssel (SCD[23]) ebenso wie die Authentisierungsreferenzdaten (SRAD[24]) des Signaturschlüssel-Inhabers befinden sich in der qualifizierten Signaturerstellungseinheit (QSEE) und werden durch diese geschützt.

3.1.2. Benutzer des EVG

3.1.2.1. Benutzer des Netzkonnektors

Die folgenden Benutzer des Netzkonnektors sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen.

In der Einsatzumgebung des Netzkonnektors gibt es folgende externe Entitäten:

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

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

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

[23] Englisch: signature-creation data

[24] Englisch: signatory reference authentication data

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

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

Für den **Leistungserbringer** sind die Leistungen des NK transparent, er arbeitet mit dem Clientsystem. Sofern er Einstellungen des NK verändert, agiert er in der Rolle des NK-Administrators. Deshalb sind Leistungserbringer bzw. HBA-Inhaber nicht gesondert als eigene externe Einheiten modelliert. Auch ein Leistungserbringer könnte grundsätzlich in der Rolle des Angreifers auftreten: Innerhalb des NK gibt es Geheimnisse (z. B. Sitzungsschlüssel des VPN-Kanals), die auch ein Leistungserbringer nicht kennen soll. Versucht ein Leistungserbringer, Kenntnis von diesen Geheimnissen zu erlangen, kann dies als Angriff betrachtet werden. Beim Leistungserbringer gilt jedoch folgende Einschränkung: Weder der NK noch der Anwendungskonnektor können gegen den Willen eines Leistungserbringers Datenschutzanforderungen durchsetzen, solange Clientsysteme dies nicht unterstützen. Daher werden solche potentiellen Angriffe eines Leistungserbringers hier **nicht** betrachtet (das Verhindern solcher Angriffe ist nicht Bestandteil der EVG-Sicherheitspolitik). Im Umfeld des Konnektors wird der Leistungserbringer als vertrauenswürdig angesehen, da er üblicherweise auch die Erfüllung des Umgebungsziels OE.NK.phys_Schutz sicherstellen muss.

3.1.2.2. Objekte des Netzkonnektors

Die folgenden Objekte des Netzkonnektors sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen.

Aus Sicht des Netzkonnektors 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 (siehe

A.NK.sichere_TI in Abschnitt 3.4.1). Die Sicherheit der Clientsysteme ist nicht Gegenstand der Betrachtung.

3.1.2.3. Benutzer des Anwendungskonnektors

Über die in Abschnitt 3.1.2.1 genannten Benutzer unterscheidet der Konnektor die folgenden Benutzer, d.h. externe Instanzen, die mit dem EVG kommunizieren (vergl. CC Teil 1 [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. [76], 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 Apothekenverwaltungssysteme der Apotheker und stellen die Anwendungsprogramme für die Leistungserbringer und Versicherten zur Verfügung. Ohne Nutzung eines TLS-Kanals kann der EVG nicht zwischen einer beliebigen Komponente im LAN und einem Clientsystem unterscheiden.	Bei Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: Öffentlicher Schlüssel Ohne Nutzung eines TLS-Kanals zwischen Clientsystem und Konnektor: keine Sicherheitsattribute
Fachmodul	Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die	**ServiceInformation:** XML-Datei zur Beschreibung der Dienste des Fachmoduls gemäß

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
	TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform.	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 Clientsystems	Der Benutzer des Clientsystems als logische Schnittstelle des EVG. Er wird durch den EVG identifiziert. Der Benutzer des Clientsystems kann durch die korrekte Authentisierung gegenüber der zu benutzenden Chipkarte für die Benutzung des EVG autorisiert werden. Die Gültigkeit einer Autorisierung kann für EVG-Funktionen in Abhängigkeit von der verwendeten Chipkarte konfiguriert werden. Für die qualifizierte elektronische Signatur muss eine Autorisierung des Benutzers für das Signieren eines jeden einzelnen Stapels der Stapelsignatur durch die qualifizierte Signaturerstellungseinheit (HBA) erfolgen.	**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	**Identität**: Umfasst die - ID.SMKT.AUT der gSMC-KT des eHealth-Kartenterminals,

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
	(s. [77] Kap. 3.7).	- physische Adresse im LAN-LE. **Authentisierungsreferenzdaten**: Authentisierungsreferenzdaten zur Authentisierung der eHealth-Kartenterminals zum Aufbau des TLS-Kanals; umfasst das Zertifikat in EF.C.SMKT.AUT der gSMC-KT, die zum Pairing benutzt wurde, und das Pairing-Geheimnis ShS.KT.AUT. **Arbeitsplatz**: Arbeitsplatz bzw. Arbeitsplätze, denen das eHealth-Kartenterminal zugeordnet ist, mit Angabe, ob es für den Arbeitsplatz lokales oder entferntes eHealth-Kartenterminal ist. Ein eHealth-Kartenterminal kann auch keinem Arbeitsplatz zugeordnet sein.
gSMC-KT	Chipkarte gSMC-KT als Sicherheitsmodule für eHealth-Kartenterminals	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel in den Zertifikaten - C.SMKT.AUT[25] als gSMC-KT. - C.SMC.AUTD_RPS_CVC[26] 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-	Keine

[25] C.SMKT.AUT steht hier für C.SMKT.AUT.R2048 und den optionalen C.SMKT.AUT.R3072 der Spezifikation des Objektsystems der gSMC-KT [85].

[26] 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 [85].

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
	Kommandos des EVG verarbeitet werden[27].	
eGK	Chipkarte, die durch den EVG identifiziert und sich gegenüber dem anderen Chipkarten mit CVC und privaten Schlüssel oder davon abgeleiteten symmetrischen Schlüsseln als eGK gegenüber CMS oder VSDM-Fachdienst authentisiert.	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: - öffentlicher Schlüssel und CHA, bzw. CHAT in dem CVC C.eGK.AUT_CVC[28] als eGK gegenüber anderen Chipkarten, - SK.CMS[29] als eGK gegenüber einem CMS, - SK.VSD[30] 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[31], Träger des Entschlüsselungsschlüssels und PIN-Empfänger.	**Identität**: - ICCSN - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten und Entschlüsselungsschlüsselinhabers für zu verschlüsselnde Daten.[32] **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten - C.HPC.AUTR_CVC[33] als HBA gegenüber SMC und eGK,

27 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.

28 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 [81].

29 SK.CMS steht hier für SK.CMS.AES128 und den optionalen SK.CMS.AES256 der Spezifikation des Objektsystems der eGK [81].

30 SK.VSD steht hier für SK.VSD.AES128 und den optionalen SK.VSD.AES256 der Spezifikation des Objektsystems der eGK [81].

31 PrK.HP.QES steht hier für PrK.HP.QES.R2048 und die optionalen PrK.HP.QES.R3076 der Spezifikation des Objektssystems [82].

32 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.

33 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 [82].

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
		- C.HPC.AUTD_SUK_CVC[34]als QSEE für Stapelsignatur und PIN-Empfänger - C.HP.ENC als Träger des dazu gehörigen Entschlüsselungs-schlüssels PrK.HP.ENC. **Optionale Authentisierungsreferenzdaten[35]:** - 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	**Identität**: ICCSN **Authentisierungsreferenzdaten mit Rollenkennung**: öffentlicher Schlüssel und ggf. CHA, bzw. CHAT in den Zertifikaten: - C.SMC.AUTR_CVC[36] als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC[37] als

[34] 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 [82].

[35] Gemäß der Spezifikation des Objektsystems des HBA [82], 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.

[36] 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 [83]

Benutzer des Anwendungskonnektors	Beschreibung	Sicherheitsattribut
	Entschlüsselungsschlüssels, Träger des privaten Signaturschlüssels, des privaten Schlüssels zur CVC-Authentisierung gegenüber der eGK und des privaten Schlüssels zur X.509-Authentisierungs-schlüssels gegenüber externen Gegenstellen verwendet werden.	SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung. **Optionale Authentisierungsreferenzdaten[38]:** - 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 Entschlüs-selungsschlüssels, Träger des privaten Signaturschlüssels, des privaten Schlüssels zur CVC-Authentisierung gegenüber der eGK und des privaten Schlüssels zur X.509-Authentisierungs-schlüssels 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[39] als SMC-B gegenüber einer eGK, - C.SMC.AUTD_RPE_CVC[40] als SMC-B und PIN-Empfänger - C.HCI.AUT X.509-Zertifikat für die Client-Server-Authentisierung,.

Tabelle 5: Benutzer des Anwendungskonnektors

[37] 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 [85] bzw. der SMC-B [83]

[38] Gemäß der Spezifikation des Objektsystems der SMC-B [83], 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 Schlüsselpaare der Karte voraus. Die symmetrische Kartenadministration erfordert einen gegenseitige Authentisierung mit MUTUAL AUTHENTICATION zwischen Karte und CMS.

[39] 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 [83]

[40] 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 [83]

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[41])
KT-Benutzer	Benutzer des eHealth-Kartenterminals.

Tabelle 6: Benutzer anderer Komponenten in der IT-Umgebung

3.2. Bedrohungen

3.2.1. Gegen den Netzkonnektor gerichtete Bedrohungen

Die folgenden Bedrohungen sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen:

3.2.1.1. Auswahl der betrachteten Bedrohungen

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

Der Netzkonnektor kann nicht verhindern, dass z. B. ein Einbrecher nachts in eine Arztpraxis eindringt und dort lokal gespeicherte medizinische Daten (z. B. Patientenakten auf Papier oder auch elektronische Patientenakten in ungeschützten Clientsystemen) entwendet – dies war auch vor Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur schon möglich. Der Netzkonnektor muss aber verhindern, dass Angreifer Zugriff auf Daten neuer Qualität oder neuer Quantität erhalten, etwa durch unbemerktes Mitlesen elektronischer Daten oder durch den unbefugten Zugriff auf Daten in der Telematikinfrastruktur. Die potentiellen Fortschritte für den Angreifer, die es zu verhindern gilt, liegen entweder

- im Datenformat (elektronische Speicherung statt Papier, da so die Kopie, Weiterverarbeitung und Auswertung stark vereinfacht wird)[42],
- in der Datenmenge (Zugriff auf Daten aller Versicherten statt Zugriff auf Daten der Versicherten nur eines Leistungserbringers (z. B. nur einer Arztpraxis), bzw. Zugriff auf alle Daten eines Versicherten (über mehrere Leistungserbringer hinweg) statt Zugriff nur auf die Daten, die bei einem Leistungserbringer über ihn vorliegen),
- in der Tatsache, dass der Zugriff nicht oder nur schwer bemerkt werden kann, so dass evtl. über lange Zeiträume hinweg unbemerkt Daten gesammelt werden können, oder

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

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

- in der Tatsache, dass der Angreifer nur einer sehr geringen Gefahr ausgesetzt ist, weil der Angriff z. B. aus dem Ausland über das Internet durchgeführt werden kann, wobei ein deutlich geringeres Risiko der Strafverfolgung besteht.

Die Einführung der Telematikinfrastruktur ist durch folgende Eigenschaften gekennzeichnet:

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

Für den Zugriff aus den lokalen Netzen der Leistungserbringer zu Diensten im Internet kann der NK als Gateway agieren[43]. Durch die Nutzung des Internet sind die Daten und Anwendungen in den lokalen Netzen Gefahren ausgesetzt, die aus den Bedrohungen im Zusammenhang mit Schwachstellen der Systeme, Anwendungen etc. und deren Benutzung resultieren. Der Schutz dieser Komponenten erfolgt nicht durch den NK, sondern durch eine Kombination von Maßnahmen in den lokalen Netzen und Systemen der Leistungserbringer (Virenscanner) mit Maßnahmen am Internet-Zugangspunkt (SIS bzw. Firewall). Im Fall der Nutzung des NK als Gateway muss dieser sicherstellen, dass die übertragenen Daten vom bzw. zum Internet ausschließlich über die Komponente SIS geroutet werden und dass die Vertraulichkeit und Integrität dieser Daten bei der Übertragung zwischen NK und SIS geschützt ist.

Dies führt zu folgenden Angriffspunkten:

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

2. Die Vertraulichkeit oder Integrität von CS-Daten, die lokal beim Leistungserbringer gespeichert sind, wird bedroht. Hier ist insbesondere der Aspekt zu erwähnen, dass die IT-Systeme des Leistungserbringers möglicherweise an unsichere Transportnetze (z. B. Internet) angeschlossen werden können und über diesen Weg Angriffe möglich sind. Der Netzkonnektor muss eine sichere Anbindung an die zentrale Telematikinfrastruktur-Plattform bereitstellen. Zudem muss der Konnektor die Verbindung zwischen dem lokalen Netzen des Leistungserbringers und dem Internet über einen Sicheren Internet Service (SIS) leiten[44].

[43] Laut Konnektor-Spezifikation (Kapitel 2.7) [76] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

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

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

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

Die wesentlichen vom Netzkonnektor abzuwehrenden Bedrohungen sind also

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

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

3.2.1.2. Liste der Bedrohungen

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

Der Anwendungskonnektor wird in dieser Abbildung nicht dargestellt, da es mehrere topologische Möglichkeiten der Anordnung des Anwendungskonnektors in Relation zum Netzkonnektor gibt (siehe auch Abbildung 2 in [69], Abschnitt 1.3.2, und Abbildung 4 in [69], Abschnitt 7.6.3). Das Kästchen „LAN-Interface“ stellt entweder die Verbindung zum

Anwendungskonnektor dar oder schützt den Anwendungskonnektor durch einen LAN-seitigen Paketfilter.

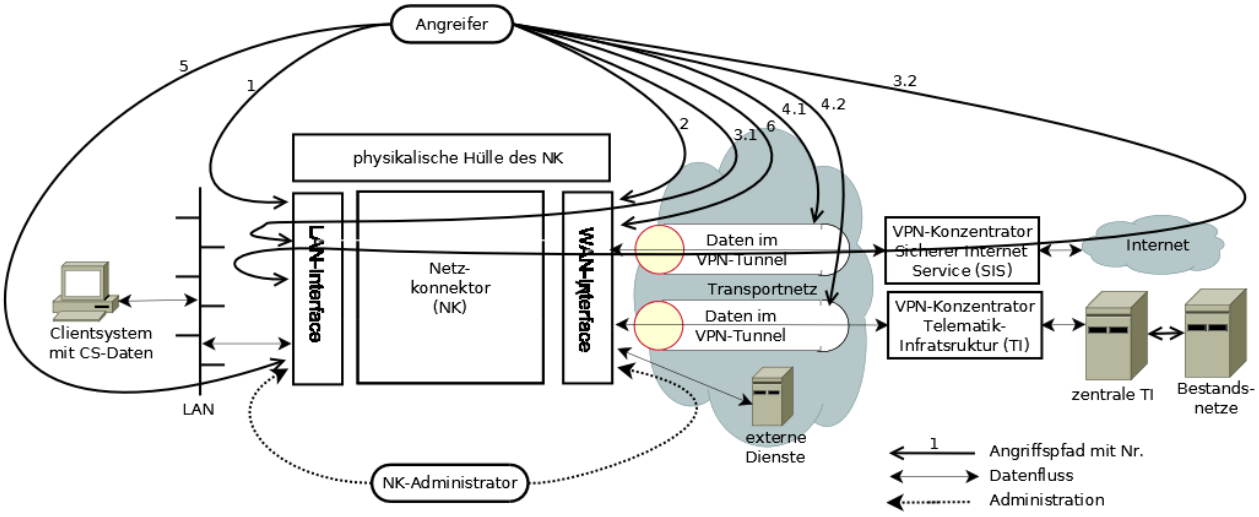


Abbildung 4: Externe Einheiten und Objekte im Zusammenhang, Angriffspfade

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

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

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

Angriffspfad	Bezeichner	Beschreibung auf Seite
Nr. 1	T.NK.local_EVG_LAN	64
Nr. 2	T.NK.remote_EVG_WAN	65
Nr. 3.1	T.NK.remote_EVG_LAN	65
Nr. 3.2	T.NK.remote_EVG_LAN	65
Nr. 4.1	T.NK.remote_VPN_Data	66
Nr. 4.2	T.NK.remote_VPN_Data	66
Nr. 5	T.NK.local_admin_LAN	66
Nr. 6	T.NK.remote_admin_WAN	67
Konnektornachbauten	T.NK.counterfeit	67
Zertifikatsstatusabfragen	T.NK.Zert_Prüf	67
Zeitsynchronisation	T.NK.TimeSync	68

Angriffspfad	Bezeichner	Beschreibung auf Seite
DNS-Manipulation	T.NK.DNS	68

Tabelle 7: Kurzbezeichner der Bedrohungen

In den folgenden Abschnitten werden die Bedrohungen genauer beschrieben.

Die Angriffe, deren Bezeichner das Wort „local“ enthalten (T.NK.local_EVG_LAN und T.NK.local_admin_LAN) nehmen an, dass der Angreifer lokal in den Räumlichkeiten des Leistungserbringers agiert, setzen also einen unbefugten physischen Zugriff auf den Netzkonnektor (z. B. Einbruch) voraus. Dabei wird angenommen, dass Personen, die berechtigten Zugang zu vor physischen Zugriff geschützten Bereichen des Leistungserbringers haben, entweder vertrauenswürdig[45] sind (so dass von ihnen keine Bedrohungen ausgehen, z. B. Arzt selbst, Servicetechniker, einige Angestellte) oder dass der physische Zugriff durch den Leistungserbringer geeignet beschränkt wird (z. B. Patienten dürfen zwar Wartezimmer und Behandlungsräume betreten, aber nicht auf den gesicherten Bereich zugreifen in welchem der Konnektor aufbewahrt wird – siehe die Annahme A.NK.phys_Schutz).

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

Die Angriffe, deren Bezeichner das Wort „admin“ enthalten (T.NK.local_admin_LAN und T.NK.remote_admin_WAN), nehmen an, dass ein Angreifer die 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.

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

Für diesen Angriff kann der Angreifer sowohl vorhandene IT-Systeme im LAN des Leistungserbringers nutzen als auch eigene (z. B. Notebook, Netbook, PDA[46], Smartphone/Handy) mitbringen.

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

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

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

T.NK.remote_EVG_WAN

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

T.NK.remote_EVG_LAN

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

Hierzu werden in Abbildung 4 zwei Angriffspfade unterschieden:

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

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

Einen Spezialfall dieses Angriffs (Angriffspfad 3.1 oder 3.2) stellt das Szenario dar, dass ein IT-System im LAN vom Transportnetz bzw. Internet (WAN) aus mit bösartigem Code

46 Personal Digital Assistant

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[47] 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
- 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 4) oder zwischen dem Konnektor und dem Sicheren Internet Service (Angriffspfad 4.1 aus Abbildung 4) 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

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

schadhafter Software, welche Kopien aller vom Netzkonnektor übertragenen Daten am VPN-Tunnel vorbei zum Angreifer spiegelt.

Diese Bedrohung umfasst auch folgende Aspekte:

Ein lokaler Angreifer bringt schadhafte Software auf den Netzkonnektor auf.

Ein lokaler Angreifer greift unautorisiert auf genutzte kryptographische Schlüssel im Arbeitsspeicher des Netzkonnektors zu.

Ein lokaler Angreifer deaktiviert die Protokollierungsfunktion des Netzkonnektors.

Ein lokaler Angreifer spielt ein Backup eines anderen Konnektors ein und überschreibt damit Daten (etwa Konfigurationsdaten).

Ein lokaler Angreifer kann mit modifizierten Konfigurationsdaten beispielsweise per dynamischem Routing den Netzwerkverkehr umleiten.

T.NK.remote_admin_WAN

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

Diese Bedrohung umfasst auch folgende Aspekte:

Ein Angreifer aus dem Transportnetz bringt schadhafte Software auf den Netzkonnektor auf.

Ein Angreifer aus dem Transportnetz greift unautorisiert auf genutzte kryptographische Schlüssel im Arbeitsspeicher des Netzkonnektors zu.

Ein Angreifer aus dem Transportnetz deaktiviert die Protokollierungsfunktion des Netzkonnektors.

T.NK.counterfeit

Ein Angreifer bringt gefälschte Netzkonnektoren in Umlauf, ohne dass dies vom VPN-Konzentrator erkannt wird[48]. 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 Netzkonnektor und einem netzbasierten Dienst (siehe OE.NK.PKI)

[48] 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.

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 Netzkonnektor 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.

T.NK.TimeSync

Ein Angreifer manipuliert Nachrichten, die im Rahmen der Zeitsynchronisation zwischen dem Netzkonnektor und einem netzbasierten Dienst (Zeitdienst) ausgetauscht werden, oder gibt sich selbst als Zeitdienst aus, um auf dem Netzkonnektor 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 schützende Daten der TI und der Bestandsnetze während der Übertragung zwischen Konnektor und zentraler Telematikinfrastruktur-Plattform bedroht. Andererseits können gefälschte DNS-Antworten auch beim Internet-Zugriff von Clientsystemen der Leistungserbringer auftreten. In einem solchen Szenario könnte der Angreifer den Zugriff der Clientsysteme auf manipluierte 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 Zeit-Dienst, kann diesen Dienst manipulieren oder verhindern. Damit wird der EVG mit gefälschten PKI- oder Zeit-Informationen versorgt oder die PKI- oder Zeit-Informationen werden komplett blockiert. Dadurch können Sicherheitsdienste des EVG, etwa die Prüfung von Zertifikaten, beeinflusst oder unterbunden werden.

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

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

T.AK.Mani.Terminal Manipuliertes Kartenterminal

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

T.AK.Mani.AdminKonsole Manipulierte Administrationskonsole

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

Betroffen sind die Management-Daten bei Übertragung zum und Verarbeitung im EVG.

3.2.2.6. Bedrohungen in den Betriebsabläufen

T.AK.MissbrauchKarte Missbrauch von Chipkarten

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

T.AK.Fehlbedienung Datenverfälschung oder Fehlkonfiguration durch Fehlbedienung

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

3.3. Organisatorische Sicherheitspolitiken

3.3.1. Organisatorische Sicherheitspolitiken des Netzkonnektors

Die in diesem Abschnitt aufgeführten organsisatorischen Sicherheitspolitiken sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen:

OSP.NK.Zeitdienst **Zeitdienst**

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

OSP.NK.SIS **Sicherer Internet Service**

Die Einsatzumgebung des Netzkonnektors 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 Netzkonnektor 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 Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74]. Zudem prüft der Netzkonnektor die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

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 organisatorischen Sicherheitspolitiken

OSP.AK.MedSoc_Data Schutz medizinischer Daten und Sozialdaten

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

OSP.AK.Konn_Spez Konformität zur Spezifikation Konnektor

Der EVG erfüllt die sicherheitsrelevanten Anforderungen des Produktsteckbriefes Konnektor [75] und der Spezifikation Konnektor [76]. 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 Schutzprofil verweist auf diese Beschreibungen soweit dies für die Festlegung von Sicherheitseigenschaften erforderlich ist. Eine Produktevaluierung gemäß Sicherheitsvorgaben, die konform zum vorliegenden Schutzprofil sind, muss aber feststellen, 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 [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74] implementiert. Für den Signaturdienst für qualifizierte elektronische Signaturen gelten die Festlegungen gemäß [9].

OSP.AK.SW-UpdateSoftware-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[49]). Schlägt die Prüfung der Integrität fehl, verhindert der EVG eine Aktualisierung der Software.

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

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

[49] Einspielen älterer Software-Versionen ist nur dann erlaubt, wenn die einzuspielende Version in der aktuell gültigen Liste zulässiger Software-Versionen (Firmware-Gruppe) ist (siehe [86]).

Prüfung nicht-qualifizierter elektronischer Signaturen und digitaler Signaturen muss den Signaturschlüssel-Inhaber, dem die Signatur zuzuordnen ist, feststellen lassen.

OSP.AK.SV_Unaltered_Data Unversehrtheit der signierten Daten

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

OSP.AK.EVG_Modification Schutz vor Veränderungen

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

3.3.2.3. Organisatorische Sicherheitspolitiken für Kryptomodul und Server

OSP.AK.Encryption Verschlüsselung und Entschlüsselung

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

OSP.AK.CardService Chipkartendienste

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

3.3.2.4. Organisatorische Sicherheitspolitiken für Fachanwendungen

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

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

dennoch eine Komponente einer Fachanwendung und/oder sein Schlüsselmaterial erfolgreich angegriffen, so werden die betroffenen Schlüssel zeitnah gesperrt.

3.4. Annahmen

3.4.1. Annahmen an den Netzkonnektor

Die folgenden Annahmen sind dem Schutzprofil BSI-CC-PP-0097 [69] entnommen:

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

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

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

Hinweis: Die Annahme A.NK.phys_Schutz an den Netzkonnektor ist identisch zur Annahme A.AK.phys_Schutz an den Anwendungskonnektors.

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

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

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

Die gSMC-K ist nach dem Schutzprofil [70] evaluiert und zertifiziert oder bietet gleichwertige Sicherheit, die zum Beispiel durch eine andere Zertifizierung außerhalb der Gesamtzertifizierung nachgewiesen werden kann. Die Gleichwertigkeit wird im Rahmen der Gesamtzertifizierung überprüft.

Anwendungshinweis 26: Siehe auch [69], Abschnitt 7.6.13.

A.NK.sichere_TI Sichere Telematikinfrastruktur-Plattform

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

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

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

Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

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

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

Anwendungshinweis 27: Siehe auch [69], Abschnitt 7.6.8.

A.NK.AK Anwendungskonnektor nutzt Netzkonnektor korrekt

Der Anwendungskonnektor nutzt die Sicherheitsdienste des Netzkonnektors über dessen Schnittstellen automatisch. Durch die Art der Aufrufe ist für den Netzkonnektor 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 ST-Autor soll die Funktionalität des Netzkonnektors und der dazu erforderlichen Separationsmechanismen beschreiben. – Siehe auch [69], Abschnitte 7.6.2 und 7.6.9.

A.NK.CS Clientsystem nutzt Netzkonnektor korrekt

Die Clientsysteme nutzen die Sicherheitsdienste des Netzkonnektors über dessen Schnittstellen automatisch. Durch die Art der Aufrufe aus dem lokalen Netz des Leistungserbringers ist für den Netzkonnektor 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 ST-Autor soll die Funktionalität des Netzkonnektors und der dazu erforderlichen Separationsmechanismen beschreiben. – Siehe auch [69], Abschnitte 7.6.2 und 7.6.9.

A.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

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

Er setzt nur nach dem vorliegenden Schutzprofil 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 Netzkonnektor 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 Netzkonnektor in der spezifizierten Art und Weise nutzen, also insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.

Er sorgt dafür, dass über Kanäle, die nicht der Kontrolle des Konnektors unterliegen (z. B. Einspielen von ausführbaren Dateien über lokale optische Laufwerke oder über USB-Stick, Öffnen von E-Mail-Anhängen) keine Schadsoftware auf die 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 Netzkonnektor 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 Netzkonnektors

Der Betreiber des Netzkonnektors sorgt dafür, dass administrative Tätigkeiten (dies umfasst sowohl die lokale als auch die optionale zentrale Administration) in Übereinstimmung mit der Administrator-Dokumentation des Netzkonnektors durchgeführt werden. Insbesondere ist für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal einzusetzen. Die Administratoren halten Authentisierungsinformationen und –token geheim bzw. geben diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token).

A.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

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

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

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

Anwendungshinweis 30: Dieser Aspekt wird im vorliegenden Schutzprofil 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 Konnektor zu konfigurieren und hat im Falle des manuellen Anwendens von Aktualisierungen das Recht das Update anzustoßen. Der Administrator hält Authentisierungsinformationen und -token geheim bzw. gibt diese nicht weiter (z. B. PIN bzw. Passwort oder Schlüssel-Token). Der Leistungserbringer als Nutzer des Konnektors hat die Verantwortung, die Eignung der aktuell genutzten Konnektorfirmware-Version zu prüfen.

Anwendungshinweis 31: Die Information der Benutzer des AKs, welche Firmware-Version aktuell genutzt wird kann auch auf technischem Wege erfolgen. In diesem Fall muss die Guidance des TOE einen entsprechenden Hinweis enthalten, dass die genutzte Firmware-Version im Primärsystem angezeigt wird. Die Guidance muss den Nutzer darüber informieren, dass er im Falle automatischer Updates die Eignung der genutzten Firmware-Version – also ob diese von der gematik zugelassen ist – prüfen muss.

Wird die Konfiguration des Parameters zur automatischen Aktualisierung der Firmware mit einem Update der Firmware auf „enabled“ geändert, muss die Guidance den Administrator darüber informieren. Ebenso muss die Guidance Hinweise enthalten, wie der Administrator – wenn er dies möchte – die Konfiguration so wieder ändern kann, ohne dass bereits ungewollt automatische Updates stattfinden (bspw. indem der Konnektor für das Installieren des Updates offline genommen und erst nach Änderung der Konfiguration zum automatischen Update wieder online genommen wird).

Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartententerminals organisatorisch genschützt werden. Dies gilt auch für ein automatisches Update. Die Guidance muss den Administrator darüber informieren, 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 [77] entsprechen und nach dem Schutzprofil für eHealth-Kartenterminals [71] evaluiert wurden.

A.AK.Konnektor Konnektor

Die Anwender/Benutzer setzen nur solche Konnektoren ein, welche der Spezifikation [76] entsprechen und nach dem Konnektor Schutzprofil BSI-CC-PP-0098 (dieses Dokument) 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

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 [80] entspricht und nach dem Schutzprofil COS Schutzprofil [70] evaluiert ist und dessen Objektsysteme der Spezifikation [83] bzw. [85] 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 nach dem Schutzprofil Card Operating System COS [70] evaluiert und zertifiziert oder bietet gleichwertige Sicherheit, die zum Beispiel durch eine andere Zertifizierung nachgewiesen werden kann.

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 [80] entspricht und nach dem Schutzprofil COS [70] evaluiert ist, deren Objektsysteme der Spezifikation [82] entspricht und das als qualifizierte elektronische Signaturerstellungseinheit nach eIDAS zertifiziert ist.

Anwendungshinweis 32: Gemäß Spezifikation [82] 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 Netzkonnektors.

4. Sicherheitsziele

4.1. Sicherheitsziele für den Netzkonnektor

Dem Schutzprofil BSI-CC-PP-0097 [69] sind folgende Sicherheitsziele für den Netzkonnektor übernommen:

4.1.1. Allgemeine Ziele: Schutz und Administration

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

Der Netzkonnektor stellt TLS-Kanäle zur sicheren Kommunikation mit anderen IT-Produkten zur Verfügung und verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74]. Zudem prüft der Netzkonnektor 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 Netzkonnektor schützt sich selbst und die ihm anvertrauten Benutzerdaten. Der Netzkonnektor schützt sich selbst gegen sicherheitstechnische Veränderungen an den äußeren logischen Schnittstellen bzw. erkennt diese oder macht diese erkennbar.

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

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

Der Netzkonnektor 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:** Im Schutzprofil [69] wird Schutz vor physischen Angriffen durch die Einsatzumgebung angenommen (siehe A.NK.phys_Schutz). Falls der Netzkonnektor aus Hardware und Software besteht, kann der ST-Autor optional fordern, dass der Netzkonnektor physische Angriffe abwehrt oder diese erkennbar macht. In diesem Fall kann die Annahme A.NK.phys_Schutz abgeschwächt werden oder entfallen. Falls der Netzkonnektor auch Schutz vor physischen Angriffen bieten soll (d.h.: falls der Netzkonnektor ein sicheres Gehäuse postuliert), umfassen die sicherheitstechnischen Veränderungen in O.NK.Schutz auch physische Manipulationen. Der ST-Autor soll in einem solchen Fall das Ziel O.NK.Schutz im Security Target geeignet erweitern. – Vergleiche zu diesem Themenkomplex auch [69], Abschnitt 7.6.7.

O.NK.EVG_Authenticity Authentizität des Netzkonnektors

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

Anwendungshinweis 35: Siehe auch [69], Abschnitt 7.6.11.

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

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

Dazu ermöglicht der Netzkonnektor die sichere Identifikation und Authentisierung (auf Basis einer in der IT-Umgebung durchgeführten Authentisierung) eines Administrators, welcher die lokale und/oder (optional) entfernte Administration des Netzkonnektors durchführen kann. Die Administration erfolgt rollenbasiert.

Weil die Administration über Netzverbindungen (lokal über PS1 oder zentral über PS2) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).

Der Netzkonnektor 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 Netzkonnektor muss mindestens die Rolle Administrator unterstützen, bei Bedarf ist auch ein abgestuftes rollenbasiertes Administrationskonzept umzusetzen (getrennte Zugangskennungen, unterschiedliche Administrationsrechte). In diesem Schutzprofil wird davon ausgegangen, dass die Authentisierung des Konnektor-Administrators vom AK vorgenommen wird. Der Netzkonnektor darf auch die Authentisierung selbst vornehmen; in diesem Fall ist O.NK.Admin_EVG geeignet zu verschärfen.

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

Anwendungshinweis 38: Der für die Administration notwendige sichere logische Kanal muss auf den durch [74] vorgegebenen Protokollen und Algorithmen beruhen.

O.NK.Protokoll Protokollierung mit Zeitstempel

Der Netzkonnektor 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 Netzkonnektor ist in die Protokollierung von Zugriffen auf medizinische Daten nicht involviert.

O.NK.Zeitdienst Zeitdienst

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

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

4.1.2. Ziele für die VPN-Funktionalität

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

Der Netzkonnektor erzwingt die Authentisierung der Kommunikationspartner der VPN-Tunnel (VPN-Konzentratoren der TI und des SIS) und ermöglicht eine Authentifizierung seiner selbst gegenüber den VPN-Konzentratoren in der zentralen Telematikinfrastruktur-Plattform und des SIS.
Der Netzkonnektor prüft zertifikatsbasiert die Authentizität der VPN-Konzentratoren der TI und des SIS.
Der Netzkonnektor authentisiert sich gegenüber den VPN-Konzentratoren der TI und des SIS. Das dazu erforderliche Schlüsselmaterial bezieht der Netzkonnektor von der gSMC-K.
Außerdem überprüft der Netzkonnektor, dass die verwendeten Algorithmen gemäß 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) [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74] noch gültig sind.

Anwendungshinweis 42: Unter Prüfung der Gültigkeit der verwendeten Algorithmen wird verstanden, dass die Einschränkungen zur Gültigkeit von Algorithmen, die bereits in [68] formuliert sind, durch den Netzkonnektor durchgesetzt werden. Beispielsweise wird in Version 1.0 des Dokuments „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)“ [68] in Abschnitt 4.5.2 gefordert, dass für die IPsec-Kommunikation zwischen Konnektor und VPN-Konzentrator „nur langfristig geeignete Kryptoalgorithmen gemäß Kapitel 3“ verwendet werden. Der Netzkonnektor soll alle in [68] formulierten Anforderungen beachten und die Verwendung der betroffenen Algorithmen geeignet beschränken. Dazu kann der Netzkonnektor Algorithmen auf Basis der Informationen der Echtzeituhr sperren (siehe OE.AK.Echtzeituhr; optional kann die Echtzeituhr auch im Netzkonnektor vorhanden sein). Alternativ kann der Netzkonnektor eine Möglichkeit zur Konfiguration der zulässigen Algorithmen anbieten und die Dokumentation des Netzkonnektors vorsehen, dass die Verwendung gewisser (nicht mehr zulässiger) Algorithmen ab dem betroffenen Zeitpunkt durch Konfiguration unterbunden wird. Ebenfalls möglich ist die organisatorische Verpflichtung der Leistungserbringer, die innerhalb des Konnektors verwendbaren Algorithmen bei Bedarf durch ein Software-Update auf die zulässige Menge zu beschränken.

O.NK.Zert_Prüf Gültigkeitsprüfung für VPN-Zertifikate

Der Netzkonnektor 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 Netzkonnektor schützt die Vertraulichkeit der Nutzdaten[50] bei der Übertragung von und zu den VPN-Konzentratoren.

Bei der Übertragung der Nutzdaten zwischen Netzkonnektor 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_IntegritätIntegritätsschutz von Daten im VPN-Tunnel

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

Bei der Übertragung der Nutzdaten zwischen Netzkonnektor und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft

[50] 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.

(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 Netzkonnektor 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[51], dann schützt der Netzkonnektor auch die Clientsysteme.

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

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

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

O.NK.PF_LAN Dynamischer Paketfilter zum LAN

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

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

Anwendungshinweis 44: Siehe auch OE.NK.AK sowie die Abschnitte 7.6.8 (Denial of Service Angriffe) und 7.6.15 (Sichere Kanäle) von [69].

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

[51] Dies ist vom Einsatzszenario und der entsprechenden Konnektor-Konfiguration abhängig, siehe [76], Kapitel 2.7.

Der Netzkonnektor 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 [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74].

O.AK.Admin Administration

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

O.AK.EVG_Modifikation Schutz vor Veränderungen

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

O.AK.Selbsttest Selbsttests

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

O.AK.Protokoll Sicherheitsprotokoll mit Zeitstempel

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

O.AK.Zeit Systemzeit

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

O.AK.Infomodell Umsetzung des Informationsmodells durch den AK

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

Anwendungshinweis 45: Das Informationsmodell des Konnektors ist in der Spezifikation [76], Kapitel 4.1.1.1 (PIC_Kon_100, Tab_Kon_507 bis Tab_Kon_510) beschrieben, Details sind dort zu entnehmen.

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

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

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

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

Der beschriebene Update-Vorgang für die Software des EVG bezieht explizit die Software des Netzkonnektors mit ein. Es steht dem Autor der Sicherheitsvorgaben frei, die Updatefunktion für Software komplett oder in Teilen durch den Netzkonnektor zu implementieren. In diesem Fall ist dieses Sicherheitsziel und die entsprechenden Sicherheitsanforderungen anzupassen und in den Sicherheitsvorgaben des Netzkonnektors zu berücksichtigen. Weiterhin steht es dem Autor der Sicherheitsvorgaben frei, die Updatefunktion für Software auch für das Nachladen von geprüften und freigegebenen Fachmodulen zu verwenden.

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[52]. Die Wohlgeformtheit der zu signierenden

[52] 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 [76] verwenden

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] [43] sowie zusätzlich für PDF/A gemäß PAdES [27] [44] und für XML zusätzlich XAdES [25] [42]. 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.

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

Der AK erlaubt die Erzeugung von digitalen Signaturen für nicht-qualifizierte elektronische Signaturen für Dokumente in den Formaten Text, PDF/A, TIFF und von binären Dokumente sowie für Binärstrings[53]. 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 [67] mit lokaler oder entfernter PIN-Eingabe. Der AK setzt die Authentisierung des Inhabers des HBAx mittels Eingabe der QES-PIN durch. Der AK steuert die Eingabe der QES-PIN am eHealth-Kartenterminal und die Erzeugung der digitalen Signatur durch den HBA für die vom autorisierten Benutzer über das Clientsystem übergebenen Daten. Bei festgestellten Abweichungen im Signaturprozess wird der Benutzer informiert und die erzeugte Signatur verworfen.

[53] 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 [76] verwenden

O.AK.Sig.Stapelsignatur Stapelsignatur

Der AK unterstützt die Erzeugung qualifizierter elektronischer Signaturen durch eine Stapelsignatur gemäß [67]. 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. [67]).

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.

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 [68] 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 [76] 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.[54] 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.

[54] 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.

O.AK.VAD Schutz der Authentisierungsverifikationsdaten

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

4.2.5. Verschlüsselungsdienste

O.AK.Enc Verschlüsselung von Daten

Der AK verschlüsselt übergebene Daten gemäß der Verschlüsselungsrichtlinie der Fachanwendung bzw. des Anwendungsfalls für die über die Schnittstelle angegeben Empfänger, wenn deren Verschlüsselungszertifikate gültig sind. Es werden die Cryptographic Message Syntax [33], XML-Encryption [21] und S/MIME [34] 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.

Fachmodule

O.AK.VSDM Versichertenstammdatenmanagement

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

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

O.AK.VZD Kommunikation mit dem zentralen Verzeichnisdienst

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

4.3. Sicherheitsziele für die Umgebung des Netzkonnektors

Aus dem Schutzprofil BSI-CC-PP-0097 [69] sind folgende Sicherheitsziele für die Umgebung des Netzkonnektors übernommen. Dabei werden einige Sicherheitsziele für die Umgebung direkt vom Gesamtkonnektor oder dessen Umgebung erfüllt. Eine Abbildung der entsprechenden Sicherheitsziele aus 4.3 findet sich in Tabelle 8: Umgang mit Umgebungszielen des NK im EVG wieder.

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

OE.NK.RNG Externer Zufallszahlengenerator

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

Anwendungshinweis 54: Es ist vorgesehen, den Zufallszahlengenerator der gSMC-K als physikalischen Zufallszahlengenerator der Klasse PTG.2 zu nutzen. Für den Fall, dass der Netzkonnektor einen eigenen DRNG bereitstellt, wurde in Abstimmung mit dem BSI eine Liste von „Approved Designs“ erstellt, um den Nachweis der Erfüllung der Anforderungen einer bestimmten Funktionsklasse nach AIS20 [6] zu vereinfachen.

Siehe auch [69], Abschnitt 7.6.12.

OE.NK.Echtzeituhr Echtzeituhr

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

Anwendungshinweis 55: In der Konnektor-Spezifikation [76] wird gefordert:

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

Eine solche Annahme ist hilfreich bei der Abschätzung, wie oft die Zeitsynchronisation erfolgen muss, um eine gewisse Genauigkeit des Zeitdienstes garantieren zu können (vgl. das Refinement zu FPT_STM.1/NK). Die Freilaufgenauigkeit garantiert eine Abweichung von weniger als 2 Sekunden pro Tag, so dass bei einer Synchronisation spätestens alle 24 Stunden der Zeitdienst des Konnektors um maximal 2 Sekunden ungenau ist.

Anwendungshinweis 56: Das Umgebungsziel des Netzkonnektors OE.NK.Echtzeituhr wurde aus dem Schutzprofil BSI-CC-PP-0097 [69] des Netzkonnektors entnommen und ist nur zur Vollständigkeit in diesem Schutzprofil enthalten. OE.NK.Echtzeituhr wird durch das Umgebungsziel OE.AK.Echtzeituhr des Anwendungskonnektors eingeschlossen. Siehe auch Tabelle 8.

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 Netzkonnektor 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

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

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

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

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

Anwendungshinweis 57: Das Betriebssystem der gSMC-K wird nach dem Schutzprofil *Common Criteria Schutzprofil (Protection Profile)* Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V3-2018, Version 2.0, 10.07.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI) [70] evaluiert und zertifiziert und das dazugehörige Objektsystem getestet. Der Hersteller des Netzkonnektors darf nur geeignete evaluierte und zertifizierte Sicherheitsmodule gSMC-K in sein Produkt integrieren. Siehe auch [69], Abschnitt 7.6.13.

OE.NK.KeyStorage Sicherer Schlüsselspeicher

Die IT-Umgebung (ein Teil des Gesamtkonnektors) stellt dem Netzkonnektor 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 Netzkonnektors, siehe FTP_ITC.1/NK.VPN_TI) oder im Rahmen des TLS-Verbindungsaufbaus (siehe FTP_ITC.1/NK.TLS). Zudem unterstützt der Schlüsselspeicher den Netzkonnektor bei der sicheren Speicherung von Geheimnissen, wie zum Beispiel Sitzungsschlüssel (session keys).

Anwendungshinweis 58: Optional kann der Schlüsselspeicher auch zur Speicherung von

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

verwendet werden.

Anwendungshinweis 59: Das Umgebungsziel des Netzkonnektors OE.NK.KeyStorage wird ganz oder teilweise durch die gSMC-K erbracht. Siehe auch Tabelle 8.

OE.NK.AK **Korrekte Nutzung des Netzkonnektors 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 Netzkonnektor übergeben, damit der Netzkonnektor 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 Netzkonnektor bereitgestellten Schnittstellen geeignet verwenden, so dass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

Anwendungshinweis 60: Siehe auch [69], Abschnitte 7.6.14 und 7.3 (VPN-Konzentrator für den Zugang zur Telematikinfrastruktur).

Anwendungshinweis 61: Das Umgebungsziel des Netzkonnektors OE.NK.AK wurde aus dem Schutzprofil BSI-CC-PP-0097 [69] des Netzkonnektors entnommen und ist nur zur Vollständigkeit in diesem Schutzprofil enthalten. Siehe auch Tabelle 8.

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 Netzkonnektors durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen und –token (z. B. PIN bzw. Passwort oder Schlüssel-Token) geheim halten bzw. dürfen diese nicht weitergeben. Wenn ein Konnektor und/oder sein Sicherheitsmodul gSMC-K gestohlen wird oder abhanden kommt, muss der Betreiber des Netzkonnektors 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: Eine eindeutige Identifikation kann z. B. über eine Seriennummer erfolgen. In diesem Fall muss organisatorisch sichergestellt werden, dass die Seriennummer bei Verlust des Gerätes noch vorliegt oder rekonstruiert werden kann, damit das Gerät bei der Verlustmeldung eindeutig identifiziert werden kann, so dass weitergehende Schritte (z. B. Sperrung des zugehörigen Zertifikats) eingeleitet werden können.

OE.NK.Admin_Auth Authentisierung des Administrators

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

Anwendungshinweis 63: Das Umgebungsziel des Netzkonnektors OE.NK.AK wurde aus dem Schutzprofil BSI-CC-PP-0097 [69] des Netzkonnektors entnommen, in dem der AK als vertrauenswürdiges Konnektorteil in der IT-Einsatzumgebung betrachtet wird. In diesem Schutzprofil wird davon ausgegangen, dass der AK die Authentisierung für den Netzkonnektor durchführt. OE.NK.AK wird daher auf das EVG-Ziel O.AK.Admin des Anwendungskonnektors abgebildet und ist nur zur Vollständigkeit enthalten. Siehe auch Tabelle 8.

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

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

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

VPN-Konzentr. sperren Wird eine Kompromittierung, Betriebsaufgabe oder Vertragsbeendigung eines VPN-Konzentrators, des Schlüsselmaterials eines VPN-Konzentrators, einer CA oder des Schlüsselmaterials einer

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

EVGs sperren

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

OE.NK.phys_Schutz Physischer Schutz des Netzkonnektors

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 materielle, organisatorische und/oder personelle 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 Netzkonnektor und weiteren Komponenten des Konnektors während aktiver Datenverarbeitung vor physischem Zugriff schützen und außerhalb aktiver Datenverarbeitung physische Manipulation erkennen.

Anwendungshinweis 64: Siehe auch [69], Abschnitt 7.6.7 und A.NK.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 8.

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 [69], Abschnitt 7.6.8.

OE.NK.Betrieb_AK Sicherer Betrieb des Anwendungskonnektors

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

sichere Admin. AK — Er administriert die Anwendungskonnektoren in sicherer Art und Weise.

Schnittstellennutzung — Er trägt die Verantwortung dafür, dass die Anwendungskonnektoren und Fachmodule den Netzkonnektor 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 [69] des Netzkonnektors entnommen und ist nur zur Vollständigkeit in diesem Schutzprofil 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 8.

OE.NK.Betrieb_CS Sicherer Betrieb der Clientsysteme

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

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

sichere Admin. CS — Er administriert die Clientsysteme in sicherer Art und Weise.

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

keine Schadsoftware — Er sorgt dafür, dass über Kanäle, die nicht der Kontrolle des Konnektors unterliegen (z. B. Einspielen von ausführbaren Dateien über lokale optische

Laufwerke oder über USB-Stick, Öffnen von E-Mail-Anhängen) keine Schadsoftware auf die Clientsysteme oder andere IT-Systeme im LAN aufgebracht wird.

Internet-Anbindung

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

Verantwortung

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

OE.NK.Ersatzverfahren Sichere Ersatzverfahren bei Ausfall der Infrastruktur

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

OE.NK.SIS Sicherer Internet Service

Die Umgebung stellt einen gesicherten Zugangspunkt zum Internet bereit. Dieser Zugangspunkt muss die dahinter liegenden Netze der Benutzer wirksam gegen Angriffe aus dem Internet schützen.[55]

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[56] 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.

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

[56] Laut Konnektor-Spezifikation (Kapitel 2.7) [76] ist ein Szenario vorgesehen, das die Verwendung eines anderen Internet-Gateways gestattet. In diesem Fall ist die Nutzung des SIS optional.

Die vorgenannten Sicherheitsziele für die Umgebung aus [69] werden im vorliegenden Schutzprofil in anderer Weise umgesetzt. Tabelle 8 enthält diese Sicherheitsziele zusammen mit der Erklärung, wie sie in diesem Schutzprofil behandelt werden.

Sicherheitsziel aus BSI-CC-PP-0097 [69]	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 [69] des Netzkonnektors entnommen und ist nur zur Vollständigkeit in diesem Schutzprofil 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	*Authentisierung des Administrators:* Dieses Sicherheitsziel wird abgebildet auf das Sicherheitsziel O.AK.Admin des Anwendungskonnektors. Dies ist konsistent zum Schutzprofil BSI-CC-PP-0097, weil der Anwendungskonnektor des vorliegenden Schutzprofiles zur Umgebung des EVG aus BSI-CC-PP-0097 gehört.
OE.NK.Betrieb_AK	*Sicherer Betrieb des Anwendungskonnektors*: Dieses Sicherheitsziel für die Umgebung des NK wird abgebildet auf die Sicherheitsziele OE.AK.Plattform und OE.AK.Personal 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.phys_Schutz sind identisch formuliert. OE.NK.phys_Schutz und OE.phys_Schutz sind ebenfalls identisch formuliert. A.NK.phys_Schutz OE.NK.phys_Schutz beziehen sich aber nur auf den Netzkonnektor als Teil des aktuellen EVG, während sich A.phys_Schutz und OE.phys_Schutz auf den gesamten EVG beziehen.
OE.NK.Echtzeituhr	Für den Konnektor wurde OE.AK.Echtzeituhr aufgenommen.

Tabelle 8: 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 kryptographischen Vorgaben aus [68] erfüllen. Die Administration der Telematikinfrastruktur sorgt dafür, dass die Server in der Telematikinfrastruktur frei von Schadsoftware gehalten werden, so dass über bestehende Kanäle zum AK keine Angriffe auf den AK erfolgen. Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

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

Fachdienste, zentrale Dienste der TI-Plattform und deren Intermediäre werden als vertrauenswürdig angesehen. Es erfolgen keine Angriffe über bestehende Kommunikationskanäle auf den AK. Die Verbindungsschlüssel auf Seiten der Fachdienste, zentralen Dienste und Intermediäre werden geheim gehalten und sind nur für die rechtmäßigen Administratoren zugänglich. Fachdienste, zentrale Dienste, Intermediäre und deren Schlüsselmaterial werden vor Angriffen geschützt. Es wird angenommen, dass nur berechtigte Entitäten über die Telematikinfrastruktur auf Fachdienste, zentrale Dienste und Intermediäre zugreifen können. Dies wird durch technische oder organisatorische Maßnahmen abgesichert. Wird dennoch ein Fachdienst/zentraler Dienst/Intermediär und/oder sein Schlüsselmaterial erfolgreich angegriffen, so werden die betroffenen Schlüssel zeitnah

gesperrt. Alle genutzten kryptographischen Sicherheitsmechanismen werden im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 [68] implementiert.

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

OE.AK.Admin_EVG Sichere Administration des Anwendungskonnektors

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

Anwendungshinweis 69: Die Information der Benutzer des AKs, welche Firmware-Version aktuell genutzt wird, kann auch auf technischem Wege erfolgen. In diesem Fall muss die Guidance des TOE einen entsprechenden Hinweis enthalten, dass die genutzte Firmware-Version im Primärsystem angezeigt wird. Die Guidance muss den Nutzer darüber informieren, dass er im Falle automatischer Updates die Eignung der genutzten Firmware-Version – also ob diese von der gematik zugelassen ist – prüfen muss.

Wird die Konfiguration des Parameters zur automatischen Aktualisierung der Firmware mit einem Update der Firmware auf „enabled“ geändert, muss die Guidance den Administrator darüber informieren. Ebenso muss die Guidance Hinweise enthalten, wie der Administrator – wenn er dies möchte – die Konfiguration so wieder ändern kann, ohne dass bereits ungewollt automatische Updates stattfinden (bspw. indem der Konnektor für das Installieren des Updates offline genommen und erst nach Änderung der Konfiguration zum automatischen Update wieder online genommen wird).

Während der Konnektor aktualisiert wird, müssen die mit dem Konnektor gepairten eHealth-Kartententerminals organisatorisch genschützt werden. Dies gilt auch für ein automatisches Update. Die Guidance muss den Administrator darüber informieren, 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 [71] evaluiert und zertifiziert sind. Dies beinhaltet insbesondere, dass das Kartenterminal

(1) die gegenseitige Authentisierung mit dem EVG und Nutzung eines TLS-Kanals für die festgelegten SICCT-Kommandos erzwingt und seine Authentisierung mit Pairing-Geheimnis unterstützt,
(2) die Kommunikation nur mit höchstens einer Gegenstelle (über höchstens einem TLS-Kanal) zum Empfang von SICCT-Kommandos und zum Senden der dazugehörigen Antworten erlaubt,
(3) dem Nutzer vom Kartenleser angezeigt wird, wenn dieser sich im sicheren PIN-Eingabemodus befindet,
(4) Kommandos zur Erzeugung geschützter Kommandos zur PIN-Prüfung, zum PIN-Wechsel und zum Rücksetzen des Fehlbedienungszählers im sicheren PIN-Modus unterstützt,
(5) die Tastatureingabedaten nur temporär im Kartenleser während der Eingabe gespeichert und nach der Übergabe an die Chipkarte wieder gelöscht werden,
(6) die gesteckten Chipkarten bei Abbau des TLS-Kanals zurücksetzt (Reset) und
(7) die Vorgaben der TR-03116-1 [68] 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

Chipkarten werden nur dann mit privaten Schlüsseln und CVC als „Secure Module Cards“ (SMC) 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 [70] 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 [68].

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 entspricht der Spezifikation [80] und ist nach dem Schutzprofil Card Operating System COS [70] evaluiert und zertifiziert oder bietet gleichwertige Sicherheit, die zum Beispiel durch eine andere Zertifizierung nachgewiesen werden kann.

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 [70] 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 [68] 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 [70] und der Spezifikation des Objektsystems [81] 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 [68] 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.Clientsystemsichere Clientsysteme

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

Alle genutzten kryptographischen Sicherheitsmechanismen werden im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 [68] 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 [76] 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 9 bildet die Bedrohungen (Threats), organisatorischen Sicherheitspolitiken (OSPs) und Annahmen (Assumptions) auf Sicherheitsziele für den Netzkonnektor und dessen Umgebung ab.

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

Bedrohung (T. ...) bzw. OSP bzw. Annahme (A. ...)	O.NK.TLS_**Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.gSMC-K	OE.NK.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.Admin_Auth	OE.NK.PKI	OE.NK.phys_Schutz	OE.NK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betrieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS
A.NK.Admin_EVG																					X									
A.NK.Ersatzverfahren																													X	
A.NK.Zugriff_gSMC-K																	X										X			

Tabelle 9: Abbildung der Sicherheitsziele des Netzkonnektors 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: Abhängig von der Ausgestaltung des Netzkonnektors kann sich die **Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen** gegenüber diesem Schutzprofil noch leicht verändern. Der ST-Autor soll die tatsächlichen Produkteigenschaften beschreiben und abhängig davon die Inhalte in Tabelle 9 und im folgenden Erklärungstext (Abschnitt 4.5.3) entsprechend anpassen.

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

Werden im Rahmen solcher Anpassungen Beziehungen ergänzt (d. h.: in Tabelle 9 werden Kreuzchen ergänzt), so ist dies kurz zu erläutern. Im Allgemeinen sollten aber keine Beziehungen (bzw. Kreuzchen) gestrichen werden (Ausnahme: Das Löschen kleiner Kreuzchen (x) in Klammern ist zulässig); falls ein großes Kreuzchen X gelöscht werden soll, so ist dies ausführlich zu begründen und mit der Zertifizierungsstelle und ggf. mit der Prüfstelle abzustimmen. Insbesondere ist darauf zu achten, dass alle Bedrohungen weiterhin vollständig und effektiv abgewehrt werden und keine leeren Zeilen oder Spalten entstehen, in denen sich nicht wenigstens ein großes Kreuzchen X befindet.

4.5.2. Überblick über die Sicherheitsziele des Anwendungskonnektors

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD	O.NK.Zeitdienst
T.AK.DTBS			x						x																			
T.AK.VAD			x			x																						
T.AK.LAN.eHKT		x	x																									
T.AK.LAN.CS																		x										
T.AK.WAN.TI																			x									
T.AK.LAN.Admin		x																										
T.AK.Kanal_Missbrauch		x	x						x									x	x				x					
T.AK.Mani.EVG					x												x			x	x	x						x
T.AK.Mani.Client																				x	x				x			x
T.AK.Mani.TI																				x	x							x
T.AK.Mani.ExternerDienst																				x	x							x
T.AK.Mani.Chipkarte																				x	x	x			x			x
T.AK.Mani.Terminal																				x	x	x			x			x
T.AK.Mani.AdminKonsole		x																		x	x							x
T.AK.MissbrauchKarte																				x	x	x		x	x			x
T.AK.Fehlbedienung																												
OSP.AK.MedSoc_Data			x				x	x		x	x		x	x	x	x		x	x				x		x			
OSP.AK.Konn_Spez		x	x			x	x	x		x		x	x							x	x	x	x	x	x			x
OSP.AK.KryptAlgo	x																											
OSP.AK.SW-Update		x																		x	x	x						x
OSP.AK.EVG_Modification					x															x	x							x
OSP.AK.SC_Sign										x	x	x	x															
OSP.AK.SC_Authorized						x			x																			
OSP.AK.SC_SVAD						x																						
OSP.AK.SC_UnalteredData									x			x	x															
OSP.AK.SV_Certificate														x														
OSP.AK.SV_Signator															x													

	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD	O.NK.Zeitdienst
y																												
OSP.AK.SV_Unaltered_Data																x												
OSP.AK.Encryption							x	x																				
OSP.AK.CardService				x		x																						
OSP.AK.Fachanwendungen																										x	x	

Tabelle 10: Abbildung der Sicherheitsziele des EVG auf Bedrohungen und OSPs

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

	OE.AK.Kartenterminal	OE.AK.Plattform	OE.AK.phys_Schutz	OE.AK.SecAuthData	OE.AK.Personal	OE.AK.HBA	OE.AK.SMC	OE.AK.eGK	OE.AK.Karten	OE.AK.PKI	OE.AK.Echtzeituhr	OE.AK.Versicherter	OE.AK.HBA-Inhaber	OE.AK.SMC-B-PIN	OE.AK.sichere_TI	OE.AK.Fachdienste	OE.AK.Admin_EVG	OE.AK.Admin_Konsole	OE.AK.Clientsystem	OE.AK.ClientsystemKorrekt	OE.AK.SW-Update	OE.AK.gSMC-K	OE.AK.Benutzer_Signatur	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro
G																									
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 11: Abbildung der Sicherheitsziele der Umgebung auf Bedrohungen, OSPs und Annahmen

4.5.3. Detaillierte Erklärung für den Netzkonnektor

4.5.3.1. Bedrohungen gegen den Netzkonnektor

T.NK.local_EVG_LAN

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

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

T.NK.remote_EVG_WAN

T.NK.remote_EVG_WAN beschreibt einen Angriff aus dem Transportnetz, bei dem der EVG bzw. dessen Integrität bedroht wird. Angriffe aus dem Transportnetz werden durch den VPN-

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

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

T.NK.remote_EVG_LAN

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

EVG erkennen, und Geheimnisse nach Benutzung aktiv gelöscht werden. Für eine sichere Speicherung der Geheimnisse sorgt OE.NK.KeyStorage.

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

Angriffe aus dem Internet über den VPN-Tunnel vom Sicheren Internet Service (siehe Angriffspfad 3.2 in Abbildung 4) werden duch die Sicherheitsfunktionalität des Sicheren Internet Service verhindert (OE.NK.SIS). Entsprechende Zugriffe werden dadurch erkannt und vor der Weiterleitung über den VPN-Tunnel zum EVG blockiert. Zusätzlich kann der LAN-seitige Packetfilter (O.NK.PF_LAN) zum Schutz des LAN und des EVG beitragen. Konnte ein LAN dennoch komprimittiert werden, schützen die LAN-seitig installierten Maßnahmen zur Erkennung und Schutz vor bösartigem Code (OE.NK.Betrieb_CS) die Clientsysteme und den EVG.

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

T.NK.remote_VPN_Data

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

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

Anwendungshinweis 73: O.NK.Protokoll (Sicherheits-Log) kann bei der Abwehr von T.NK.remote_VPN_Data unterstützen, indem auch sicherheitsrelevante Ereignisse im Zusammenhang mit dem VPN-Client protokolliert werden (Schreiben von Sicherheits-Log-Daten zur späteren Auswertung oder forensischen Analyse nach einem Angriff). Siehe auch Anwendungshinweis 72.

T.NK.local_admin_LAN

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

Anwendungshinweis 74: Optional kann auch der Paketfilter gemäß O.NK.PF_LAN bzw. O.NK.PF_WAN und entsprechend die *stateful packet inspection* gemäß O.NK.Stateful zur Abwehr von T.NK.local_admin_LAN bzw. T.NK.remote_admin_WAN beitragen. Ebenfalls optional kann eine PKI in der IT-Einsatzumgebung (OE.NK.PKI) genutzt werden, um den sicheren Kanal für die Administration aufzubauen. Falls im Rahmen der Administration kryptographische Verfahren zum Einsatz kommen (z. B. im Rahmen der Benutzerauthentisierung oder bei der Implementierung eines sicheren Kanals), trägt auch OE.NK.Ersatzverfahren zur Abwehr von T.NK.local_admin_LAN bei. Schließlich kann auch OE.NK.phys_Schutz zur Abwehr von T.NK.local_admin_LAN beitragen, falls durch den Schutz des Kommunikationskanals zwischen dem EVG und weiteren Komponenten des Konnektors Manipulationen am Gerät verhindert werden können. Siehe auch Anwendungshinweis 72 (Anpassung des Security Targets bei Bedarf).

T.NK.remote_admin_WAN

T.NK.remote_admin_WAN betrachtet Angriffe im Zusammenhang mit zentraler Administration. Der Unterschied im Angriffspfad zwischen T.NK.remote_admin_WAN und T.NK.local_admin_LAN besteht darin, dass der Angreifer bei T.NK.remote_admin_WAN aus dem Transportnetz heraus versucht, seinen Angriff durchzuführen, während bei T.NK.local_admin_LAN die Angriffsversuche aus dem lokalen Netz heraus durchgeführt werden. Bei der Abwehr sind jedoch die gleichen Mechanismen beteiligt (Zugriffskontrolle, Authentisierung des Administrators, Selbstschutz, Protokollierung) und diese wirken unabhängig vom Ursprungsort des Angriffsversuchs, daher gilt hier sinngemäß das gleiche wie unter T.NK.local_admin_LAN und Anwendungshinweis 74 Zur Abwehr tragen die Ziele O.NK.Admin_EVG, OE.NK.Admin_Auth, OE.NK.Admin_EVG, OE.NK.RNG, O.NK.Protokoll, O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro, O.NK.Schutz und OE.NK.KeyStorage bei sowie optional auch OE.NK.PKI und OE.NK.Ersatzverfahren. Optional wirkt auch der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful gegen diese Bedrohung, siehe auch Anwendungshinweis 74.

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: Optional kann es im Rahmen der Gültigkeitsprüfung von Zertifikaten Plausibilitätsprüfungen geben, welche die Echtzeit des EVG verwenden; somit kann auch O.NK.Zeitdienst, OE.NK.Echtzeituhr, OE.NK.Zeitsynchro zur Abwehr von T.NK.Zert_Prüf beitragen. Optional können auch O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr von T.NK.Zert_Prüf beitragen. Zum Aufbau des sicheren Kanals zu den Netzdiensten werden Schlüssel verwendet, die in der gSMC-K gespeichert sind, daher kann OE.NK.gSMC-K optional bei der Abwehr von T.NK.Zert_Prüf unterstützen. Ein externer Zufallszahlengenerator (OE.NK.RNG) wird darüber hinaus als Lieferant für gute Zufallszahlen genutzt, die im Rahmen eines Challenge-Response-Protokolls zum Einsatz kommen können. Das Security Target ist entsprechend anzupassen, siehe Anwendungshinweis 72.

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: Auch bei T.NK.TimeSync können optional O.NK.Protokoll und der Paketfilter gemäß O.NK.PF_WAN und entsprechend O.NK.Stateful zur Abwehr der Bedrohungen beitragen. Das Security Target ist entsprechend anzupassen, siehe Anwendungshinweis 72.

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

Im Fall einer DNS-Auflösung durch Clientsysteme beim Zugriff auf das Internet führt die Manipulation der DNS-Antwort dazu, dass Clientsysteme auf Seiten umgelenkt werden können, die nicht ihrer ursprünglichen Intention entsprechen. Erfolgt dies vom Benutzer unbemerkt, können bei bösartigen Systemen die Clientsysteme durch bösartigen Code infiziert werden. Dies kann einerseits durch Erkennungsmechanismen im SIS verhindert werden, welches wirksame Maßnahmen gegen Angriffe aus dem internet implementieren soll (OE.NK.SIS). In jedem Fall muss der bösartige Code auf den Clientsystemen aber durch Mechanismen auf den Clientsystemen (Einsatz von sicheren Produkten und Virenscannern) erkannt und neutralisiert werden (OE.NK.Betrieb_CS).

4.5.3.2. Organisatorische Sicherheitspolitiken für den Netzkonnektor

OSP.NK.Zeitdienst

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

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

OSP.NK.SIS

[57] 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.

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

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

OSP.NK.BOF

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

OSP.NK.TLS

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

4.5.3.3. Annahmen des Netzkonnektors

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

Die Annahme A.NK.Zugriff_gSMC-K lautet:

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

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

OE.NK.gSMC-K impliziert, dass eine gSMC-K existiert und nach einem entsprechenden Schutzprofil evaluiert und zertifiziert ist, und dass der EVG Zugriff auf dieses Modul hat. Der Hersteller des EVG verbaut nur solche zertifizierten Module und die gSMC-K ist sicher mit dem EVG verbunden, so dass die Kommunikation zwischen gSMC-K und EVG weder

mitgelesen noch manipuliert werden kann. Somit müssen im Rahmen der Zugriffskontrolle überhaupt nur Zugriffe anderer Konnektorteile (AK) auf die gSMC-K betrachtet werden.

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

4.5.4. Detaillierte Erklärung für den Anwendungskonnektor

4.5.4.1. Bedrohungen

T.AK.DTBS

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

T.AK.VAD

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

T.AK.LAN.eHKT

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

T.AK.LAN.CS

Die Bedrohung T.AK.LAN.CS beschreibt Angriffe auf die Integrität und Vertraulichkeit der im LAN zwischen dem EVG und Clientsystemen übertragenen Daten. Das Sicherheitsziel O.AK.LAN schützt gegen Abhören, Fälschen und Vorgeben einer falschen Identität bei der Kommunikation mit den Clientsystemen im LAN der Leistungserbringer. Bei der Gegenstelle der Kommunikation ist ein ebenso vertrauenswürdiger Umgang mit den übertragenen Daten und mit dem genutzten Schlüsselmaterial erforderlich. Dies wird mit dem Sicherheitsziel OE.AK.Clientsystem erreicht.

T.AK.WAN.TI

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

T.AK.LAN.Admin

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

T.AK.Kanal_Missbrauch

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

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

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

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

T.AK.Mani.EVG

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

T.AK.Mani.Client

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

T.AK.Mani.TI

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

T.AK.Mani.ExternerDienst

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

T.AK.Mani.Chipkarte

Manipulierte Chipkarten werden durch die Bedrohung T.AK.Mani.Chipkarte betrachtet. Die eingesetzten Chipkarten sind gemäß OE.AK.SMC, OE.AK.HBA, OE.AK.eGK, OE.AK.gSMC-K evaluiert und zertifiziert und verfügen somit über entsprechende Schutzmechanismen, die Manipulationen wirksam verhindern. Gemäß OE.AK.Karten werden gefälschte Chipkarten in Kartenlesern des LAN des Leistungserbringers erkannt bzw. die Verarbeitung ungesicherter persönlicher Daten der Chipkarten verhindert. Die gSMC-K ist gemäß BSI-CC-PP-0082 zertifiziert und verfügt damit ebenfalls über entsprechende Schutzmechanismen. Der EVG bietet mit der Nutzung einer PKI (OE.AK.PKI) Möglichkeiten zum Zurückziehen von Kartenzertifikaten, die eine weitere Nutzung der betroffenen Identitäten auf den Chipkarten verhindern. Dies wird insbesondere durch die Sicherheitsziele O.AK.Update und O.AK.Infomodell erreicht: Durch O.AK.Update werden dem EVG entsprechende Listen über den Status von Identitäten geliefert, die für die Zuordnung der einzelnen Komponenten im Betrieb des EVG im Sinne des Informationsmodells benötigt werden. Abweichungen vom Informationsmodell werden durch O.AK.Infomodell nicht akzeptiert, durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr, O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.Mani.Terminal

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

T.AK.Mani.AdminKonsole

Die Bedrohung T.AK.Mani.AdminKonsole betrachtet manipulierte Administrationskonsolen, um unautorisiert Veränderungen am EVG vorzunehmen oder Zugriff auf zu schützende Daten zu erlangen. Die wird durch OE.AK.Admin_Konsole verhindert, wobei eine sichere

Administrationskonsole gefordert wird. Zudem fordert das Sicherheitsziel O.AK.Admin entsprechende Mechanismen, die nur erfolgreich authentisierten Administratoren Zugriff zu administrativen Funktionen des EVG erlauben. Erkannte Verstöße werden durch O.AK.Protokoll protokolliert und durch O.AK.Zeit (mit Hilfe von OE.AK.Echtzeituhr O.NK.Zeitdienst, OE.NK.Echtzeituhr und OE.NK.Zeitsynchro) mit einem sicheren Zeitstempel versehen.

T.AK.MissbrauchKarte

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

T.AK.Fehlbedienung

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

4.5.4.2. Organisatorische Sicherheitspolitiken

OSP.AK.MedSoc_Data

Die Sicherheitspolitik OSP.AK.MedSoc_Data verlangt, Dienste zur qualifizierten und nichtqualifizierten elektronischen Signatur, zur Chiffrierung von Dateien sowie zur kryptographischen Absicherung der Kommunikation bereitzustellen. Dadurch wird die Vertraulichkeit und Integrität aller Daten, die durch oder an die Telematikinfrastruktur, ein Clientsystem des Leistungserbringers oder eine elektronische Gesundheitskarte übergeben werden, gewährleistet. Die Sicherheitsziele des EVG tragen dem wie folgt Rechnung:

- O.AK.Sig.SignNonQES, O.AK.Sig.Stapelsignatur und O.AK.Sig.SignQES fordern die Bereitstellung von Signaturdiensten für die Erstellung nichtqualifizierter

elektronischer Signaturen mit der SMC-B (s. OE.AK.SMC) und qualifizierter elektronischer Signaturen mit dem HBA als QSEE (s. OE.AK.HBA),

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

OSP.AK.Konn_Spez

Die Sicherheitspolitik OSP.AK.Konn_Spez fordert die Erfüllung der sicherheitsrelevanten Anforderungen der Konnektor-Spezifikation [76] und die Durchsetzung der zulässigen Signaturrichtlinien und Verschlüsselungsrichtlinien. Die EVG-Sicherheitsziele O.AK.Admin, O.AK.IFD-Komm (Kommunikation mit eHealth-Kartenterminals), O.AK.Enc, O.AK.Dec, O.AK.Sig.SignQES, O.AK.Sig.Einfachsignatur, O.AK.Sig.Stapelsignatur, O.AK.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 [76] um (und andere EVG-Sicherheitsziele präzisieren diese). Die Durchsetzung zulässiger Signaturrichtlinien wird explizit in O.AK.Sig.SignQES und für Verschlüsselungsrichtlinien in O.AK.Enc gefordert, deren Bereitstellung durch OE.AK.PKI gewährleistet wird. Das Sicherheitsziel OE.AK.Echtzeituhr (mit Hilfe von O.NK.Zeitdienst und OE.NK.Echtzeituhr) deckt die Anforderungen der Konnektor-Spezifikation zur Verwendung von Echtzeit ab. Die spezifizierten Abläufe und Zuordnungen zwischen dem EVG und externen Komponenten werden durch O.AK.Infomodell im EVG implementiert.

OSP.AK.KryptAlgo

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

zertifizierter Komponenten sichergestellt. Dies drückt sich in den Sicherheitszielen für die Einsatzumgebung OE.AK.Kartenterminal, OE.AK.HBA, OE.AK.SMC und OE.AK.eGK aus.

OSP.AK.SW-Update

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

OSP.AK.EVG_Modification

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

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

und unter den Bedingungen der Sicherheitsziele für die Einsatzumgebung

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

geeignet umgesetzt.

OSP.AK.SC_Sign

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

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

OSP.AK.SC_Authorized

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

- O.AK.Sig.exklusivZugriff fordert, dass der EVG nur für solche Dateien und Heilberufsausweise den Signaturprozess auslösen darf, die von dem autorisierten Benutzer des Clientsystems ausgewählt wurden (Stapel). Die Autorisierung basiert auf einer erfolgreichen Authentisierung des Benutzers des Clientsystems als Signaturschlüssel-Inhaber, die nach OE.AK.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 und O.AK.Sig.Stapelsignatur umgesetzt.

OSP.AK.SV_Certificate

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

OSP.AK.SV_Signatory

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

OSP.AK.SV_Unaltered_Data

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

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

OSP.AK.Encryption

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

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

OSP.AK.CardService

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

OSP.AK.Fachanwendungen

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

4.5.4.3. Annahmen

- Die Annahme A.AK.Cardterminal_eHealth wird durch das Umgebungsziel OE.AK.Kartenterminal geeignet umgesetzt.
- Die Annahme A.AK.Konnektor wird durch das Umgebungsziel OE.AK.Plattform geeignet umgesetzt.
- Die Annahme A.AK.Versicherter wird offensichtlich durch das Umgebungsziel OE.AK.Versicherter abgebildet.
- Die Annahme A.AK.HBA-Inhaber wird offensichtlich durch das Umgebungsziel OE.AK.HBA-Inhaber abgebildet.
- Die Annahme A.AK.SMC-B-PIN wird offensichtlich durch das Umgebungsziel OE.AK.SMC-B-PIN abgebildet.
- Die Annahme A.AK.sichere_TI wird offensichtlich durch das Umgebungsziel OE.AK.sichere_TI abgebildet.
- Die Annahme A.AK.Admin_EVG wird offensichtlich durch das Umgebungsziel OE.AK.Admin_EVG abgebildet.
- Die Annahme A.AK.SMC wird durch das Umgebungsziel OE.AK.SMC geeignet umgesetzt.
- Die Annahme A.AK.QSCD wird durch das Umgebungsziel OE.AK.HBA geeignet umgesetzt.

- Die Annahme A.AK.phys_Schutz wird durch das Umgebungsziel OE.AK.phys_Schutz geeignet umgesetzt.
- Die Annahme A.AK.Chipkarteninhaber wird durch die Umgebungsziele OE.AK.Personal in Bezug auf die Vertrauenswürdigkeit im Umgang mit den ihm anvertrauten zu schützenden Daten und OE.AK.SecAuthData im Bezug auf den Schutz seiner Authentisierungsdaten geeignet umgesetzt.
- Die Annahme A.AK.Benutzer_Signatur wird durch das Umgebungsziel OE.AK.Benutzer_Signatur geeignet umgesetzt.
- Die Annahme A.AK.gSMC-K wird durch das Umgebungsziel OE.AK.gSMC-K geeignet umgesetzt.
- Die Annahme A.AK.Env_Arbeitsplatz wird durch die Umgebungsziele OE.AK.Clientsystem und OE.AK.ClientsystemKorrekt umgesetzt.

5. Definition 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 Card Operating System (PP COS) [70], 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*].

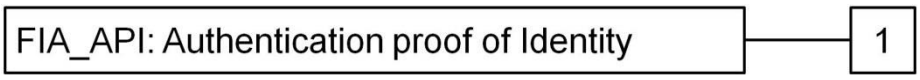
FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

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

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

Die Auswahl der funktionalen Sicherheitsanforderungen basiert auf der zum Zeitpunkt der Erstellung des Schutzprofils aktuellen Version 3.1 Revision 5 der Common Criteria; diese Version [2] liegt in englischer Sprache vor. Daher wurden in diesem Schutzprofil die Formulierungen an Common Criteria Version 3.1 Revision 5 in deutscher Sprache angepasst.

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

Sicherheitsziele des Netzkonnektors

Die durchgeführten Operationen auf die funktionalen Sicherheitsanforderungen in Kapitel 6.2 sind wie folgt kenntlich gemacht:

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

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

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

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

Sicherheitsziele des Anwendungskonnektors

Die durchgeführten Operationen auf die funktionalen Sicherheitsanforderungen in Kapitel 6.3 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 Schutzprofil 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 Schutzprofil 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 diesem Schutzprofil werden Iterationen durch einen Schrägstrich „/“ und den Iterationsidentifikator hinter dem Komponentenidentifikator angegeben.

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Dieses Schutzprofil betrachtet für jeden in Tabelle 5 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 5 definiert.

6.1.2.1. Subjekte

Subjekt	Beschreibung	Sicherheitsattribut
S_Administrator	Subjekt, das für einen Administrator handelt.	Siehe Tabelle 5.
S_Signaturdienst	Dienst des EVG zur Erstellung und Prüfung qualifizierter und	Das Subjekt übernimmt die Sicherheitsattribute des

Subjekt	Beschreibung	Sicherheitsattribut
	nichtqualifizierter elektronischer Signaturen	aufrufenden Benutzers
S_Verschlüsselungsdienst	Dienst des EVG zur Verschlüsselung und Entschlüsselung von Dokumenten	Kein Sicherheitsattribut
S_Chipkarten-dienst	Dienst des EVG zur Verwaltung und zum Zugriff auf gesteckte Chipkarten	Kein Sicherheitsattribut
S_Kartenterminaldienst	Dienst des EVG zur Verwaltung und zum Zugriff auf eHealth-Kartenterminals	Kein Sicherheitsattribut
S_TSL_Dienst	Zentraler TSL-Dienst der TI nach [87]. 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 Sicherheits-attribut gibt an, ob der Aufruf durch ein Clientsystem oder ein Fachmodul erfolgte.
S_NK	Subjekt, das für einen Prozess des NK handelt.	Kein Sicherheitsattribut
S_Benutzer_Clientsystem	Subjekt, das für den Benutzer des Clientsystems handelt. Der Benutzer wird durch den EVG identifiziert, und die korrekte Authentisierung gegenüber der zu benutzenden Chipkarte autorisiert. Im Fall der Stapelsignatur für die qualifizierte elektronische Signatur muss eine Autorisierung des Benutzers für das Signieren eines jeden einzelnen Dokuments bei Einfachsignatur oder eines Stapels bei der Stapelsignatur erfolgen.	**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,

Subjekt	Beschreibung	Sicherheitsattribut
		- „autorisiert“: Zuordnung durch Chipkarte bestätigt.
S_eHKT	Subjekt des eHealth-Kartenterminals, das mit dem eHealth-Kartenterminal kommuniziert. eHealth-Kartenterminals besitzen mindestens 1 ID-000 Kartensteckplatz und mindestens 1 ID-1 Kartensteckplatz zur Aufnahme von Chipkarten.	**Identität**: Umfasst die - ID.SMKT.AUT des eHealth-Kartenterminals, - physische Adresse im LAN-LE. **Arbeitsplatz**: zugeordneter Arbeitsplatz des eHealth-Kartenterminals. **Kartenslot**: Adresse des Kartenslots und die darin gesteckte Chipkarte. **Authentisierungsstatus**: - „nicht identifiziert“ – Kartenterminal unbekannter Identität ohne vereinbarte Pairing-Geheimnis - „identifiziert“ – Identität des eHealth-Kartenterminals ist bekannt, Pairing-Geheimnis bekannt, - „authentisiert“ – erfolgreiche Authentisierung mit der SMC als gSMC-KT und mit Pairing-Geheimnis, bestehender TLS-Kanal
S_HBA	Subjekt, das einem HBA in einem Chipkartensteckplatz eines eHealth-Kartenterminals zugeordnet ist	**Identität**: - ICCSN, - eindeutige Referenz des Signaturschlüssel-Inhabers für die zu signierenden Daten - eindeutige Referenz des Entschlüsselungsschlüssel-inhabers für verschlüsselte Daten.[58] **Kartenhandle**: identifiziert den HBA in einem

[58] 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
		Chipkartensteckplatzeines eHealth-Kartenterminals.
S_gSMC-KT	Subjekt, das einer Chipkarte gSMC-KT in einem Chipkarten-steckplatz eines eHealth-Karten-terminals 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 Entschlüsselungsschlüssel-inhabers für verschlüsselte Daten.[59] **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	**Identität:**

[59] 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
	Fachmodul agiert. Fachmodule sind Teile von Fachanwendungen die auf dem Konnektor ablaufen (siehe auch Fachmodul im Glossar).	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
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 [88]. Der VZD Enthält Einträge von Leistungserbringern und	Kein Sicherheitsattribut

Subjekt	Beschreibung	Sicherheitsattribut
	Institutionen mit allen definierten Attributen.	
S_Benutzern	Menge der folgenden Subjekte: a) S_AK b) S_Signaturdienst c) S_Benutzer_Clientsystem	Siehe entsprechende Attribute der einzelnen Subjekte.

Tabelle 12: Subjekte

6.1.2.2. Objekte

Dieses Schutzprofil 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 [80]).
SICCT-Kommando	Kommandos zur Steuerung der eHealth-Kartenterminals. Die SICCT-Kommandos dienen [77] [79] - der Steuerung des eHealth-Kartenterminals, insbesondere zur Kommunikation mit dem Konnektor, Kommandoabarbeitung und	**Typ des SICCT-Kommandos**: - eHKT-Steuerungskommando, - Benutzerkommuikationskommando, - Chipkartenkommando, - PIN-Prozesskommando.

Objekt	Beschreibung	Sicherheitsattribut
	Konfiguration der eHealth-Kartenterminals (hier kurz „eHKT-Steuerungskommando“ genannt), - dem Zugriff auf die Anzeige (Display und Anzeige des gesicherten PIN-Modus), und die Tastatur (lesend) sowie ggf. dem Tongeber (hier kurz „Benutzer-kommuikationskommando“ genannt), - der Kontrolle, Aktivierung, Deaktivierung und Statusabfrage des elektrischen Zustands von Chipkartenkontaktiereinheiten und der Kommunikation mit Chipkarten in den Chipkartenslots (hier kurz „Chipkartenkommando“ genannt), und - die Auslösung der Prozesse zur PIN-Eingabe und dem PIN-Wechsel im gesicherten Modus (hier kurz „PIN-Prozesskommando“ genannt).	
Antwort auf SICCT-Kommando	Antwortnachricht des eHealth-Kartenterminals auf ein zuvor gesendetes SICCT-Kommando, siehe [79].	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	**Autorisierungsstatus:** Status der Auswahl der Daten zur Erstellung einer qualifizierten elektronischen Signatur: - „nicht autorisiert“: Auswahl nicht durch Signaturschlüssel-Inhaber bestätigt - „autorisiert“: Auswahl durch

Objekt	Beschreibung	Sicherheitsattribut
	zum signieren übertragen werden. Die Vertraulichkeit und Integrität zu signierender Dokumente ist zu schützen[60].	Signaturschlüssel-Inhaber bestätigt. **Signaturrichtlinie:** Beschreibung der Regeln, welche Signatur (qualifiziert, nichtqualifizierte) zu erstellen ist, die signierten Dokumente zu formatieren und – im Fall der QES – wie die Daten darzustellen sind.
Signaturstapel	Ein Stapel zu signierender Daten, der (nach erfolgreicher Authentisierung des Signaturschlüsselinhabers mit der Signatur-PIN gegenüber der Signaturchipkarte) durch den Signaturdienst an die Signaturkarte zum Signieren gesendet wird.	Kein Sicherheitsattribut
Signierte Dokumente	Daten, denen eine digitale Signatur zugeordnet ist. Die Vertraulichkeit signierter Daten ist zu schützen[61]. 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

[60] 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.

[61] Der EVG schützt die Vertraulichkeit signierten Dokumente, da diese im allgemeinen Fall medizinische Daten sein können und keine explizite Aussage über einen ausschließlichen Schutz der Integrität getroffen werden kann.

Objekt	Beschreibung	Sicherheitsattribut
		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[62].	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 Benutzern gegenüber anderen Instanzen übergeben werden.	Kein Sicherheitsattribut
Signierter Bitstring	Von den Chipkarten empfangene digitale Signaturen von Bitstrings, die als zu signierende Bitstrings dem EVG übergeben wurden.	Kein Sicherheitsattribut
Zu verschlüsselnde Daten	Klardaten, die für identifizierte Empfänger verschlüsselt werden sollen. Die Klardaten und die Empfänger werden vom Aufrufenden dem EVG übergeben und die verschlüsselten Daten an den Aufrufenden zurückgegeben.	**Objekt-ID:** eindeutige Identität der zu verschlüsselnden Daten. **Vorgeschlagene Empfänger:** Identität der Empfänger der zu verschlüsselnden Daten, die vom Aufrufenden (auch zum Auffinden

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

Objekt	Beschreibung	Sicherheitsattribut
	Die Vertraulichkeit dieser Klardaten ist zu gewährleisten.	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 Verschlüs-selungszertifikate 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 entschlüs-selten Klardaten einschließlich der	**Vorgeschlagene Empfänger:** Identität der Empfänger, für den die Daten entschlüsselt werden, und an den die Daten übergeben werden sollen. **Verschlüsselungsrichtlinie:** siehe Beschreibung zur

Objekt	Beschreibung	Sicherheitsattribut
	kryptographischen Schlüssel ist innerhalb der Kontrolle des EVG zu gewährleisten.	Verschlüsselungsrichtlinie im Glossar
Entschlüsselte Daten	Entschlüsselte Daten, die für einen Benutzer entschlüsselt wurden. Die entschlüsselten Klardaten werden an den Aufrufenden zurückgegeben. Die Vertraulichkeit der entschlüsselten Klardaten einschließlich der kryptographischen Schlüssel ist 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 [81],	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[63]	Kein Sicherheitsattribut
Authentisierungs-verifikationsdaten (VAD)	Datum, das vom Benutzer zum Nachweis seiner Identität gegenüber Chipkarten dient. Dies sind VAD der Kartenhalter und die SVAD[64] als Signaturschlüssel-Inhaber gegenüber der	Kein Sicherheitsattribut

63 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.

64 Englisch: signatory verification authentication data.

Objekt	Beschreibung	Sicherheitsattribut
	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[65]. Die Vertraulichkeit und Integrität[66] der VAD müssen geschützt werden.	
Authentisierungs-referenzdaten der Identität „SAK“	Kartenprüfbares Zertifikat C.SAK.AUTD_CVC, welches von dem EVG zum Nachweis seiner Identität gegenüber dem HBA und der SMC präsentiert wird und den öffentlichen Schlüssel PuK.SAK.AUTD_CVC enthält, der zum privaten Schlüssel PrK.SAK.AUTD_CVC korrespondiert.	Kein Sicherheitsattribut
Authentisierungs-referenzdaten des AK	Kartenprüfbares Zertifikat C.SAK.AUT, welches von dem AK zum Nachweis seiner Identität gegenüber den eHealth-Kartenterminals[67] 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	Kein Sicherheitsattribut

65 Der Heilberufsausweis als qualifizierte Signaturerstellungseinheit unterstützt nur die Authentisierung durch Wissen.

66 Der Schutz der Integrität ist insbesondere bei einem Wechsel der SVAD erforderlich.

67 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
	einer anderen Komponente der Telematikinfrastruktur an den Konnektor übertragen werden. Die empfangenen Daten werden entschlüsselt und integritätsgeprüft. Es werden unverfälscht empfangene Daten ausgegeben.	
Datenobjekte des sicheren Datenspeichers (Datenobjekt des SDS)	Datenobjekte, die im sicheren Datenspeicher gespeichert sind.	**Administrator**: Werte „Administratorobjekt“ und „allgemeines Datenobjekt“
Schlüssel für sicheren Datenspeicher	Der Zugriff auf den Inhalt des sicheren (geschützten) Datenspeichers durch den Konnektor ist durch Nutzung von Schlüsselmaterial abgesichert. Datenobjekte im sicheren Datenspeicher dürfen nur verschlüsselt gespeichert werden.	Kein Sicherheitsattribut
eHealth-Kartenterminal	Ein im LAN des Leistungserbringers vorhandenes und gepaartes eHealth-KT	**Arbeitsplatz**: zugeordneter Arbeitsplatz des eHealth-Kartenterminals: • eindeutige Identifikation • erlaubte Zuordnungen als lokales KT zu einem Arbeitsplatz • erlaubte Zuordnungen als entferntes KT zu einem Arbeitsplatz • erlaubte Zuordnungen als entferntes PIN-Eingabe-KT für eine Kombination aus Mandant und Arbeitsplatz • erlaubte Zuordnungen zu einem Mandanten
Kartensitzung eGK	Kartensitzung einer eGK	Für jede eGK-Kartensitzung: • Bindung an den Arbeitsplatz, von dem aus zuerst auf die eGK zugegriffen wurde • Karte, welche die eGK im Rahmen einer Card-to-

Objekt	Beschreibung	Sicherheitsattribut
		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 Konnektor verwalteten externen Ressourcen (Kartentermi-nal mit Slots, Arbeitsplatz mit Signaturproxy und SMC-Bs)	Kein Sicherheitsattribut

Objekt	Beschreibung	Sicherheitsattribut
	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. [76], 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

Tabelle 13: zusätzliche Objekte

Die Operationen der Subjekte auf Objekte sind in den Tabellen Tabelle 15, Tabelle 16, Tabelle 17, Tabelle 18, Tabelle 19 und Tabelle 21 nach den jeweiligen Komponenten FDP_ACF definiert.

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 Verschlüsselungs zertifikate (CA certificates of an encryption PKI)	Öffentliche Schlüssel einer Sub-CA, die Zertifikate für die Verschlüsselung von Daten erstellen. Der EVG kann einen oder mehrere dieser öffentlichen Schlüssel speichern. Die Verteilung dieser Schlüssel erfolgt durch die TSL. Die Integrität dieses Schlüssels bzw. dieser Schlüssel ist zu schützen.
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	Privater Schlüssel PrK.SAK.AUTD_CVC, welcher von der SAK zum Nachweis ihrer Identität gegenüber dem HBA benutzt wird und zum

TSF Datum	Beschreibung
der Identität „SAK“.	öffentlichen Schlüssel PuK.SAK.AUTD_CVC im Zertifikat C.SAK.AUTD_CVC korrespondiert.
Authentisierungs-verifikationsdaten der AK	Privater Schlüssel PrK.SAK.AUT, welcher von dem AK zum Nachweis seiner Identität gegenüber den eHealth-Kartenterminals benutzt wird und zum öffentlichen Schlüssel PuK.SAK.AUT im Zertifikat C.SAK.AUT korrespondiert.
Authentisierungs-referenzdaten der eHealth-Karten-terminals	Identität für die Identifizierung und Authentisierungsreferenzdaten (Pairing-Daten) für die Authentisierung jedes mit dem AK gepaarten eHealth-Kartenterminals.
Authentisierungs-referenzdaten des Administrators	Identität für die Identifizierung und Authentisierungsreferenzdaten für die Authentisierung des Administrators.
Identität des Arbeitsplatzes	Identität des Arbeitsplatzes des Benutzers für die Anforderung von Sicherheitsdiensten des EVG, die vom Clientsystem an den EVG übergeben wird.
Arbeitsplatz-konfigurations-daten	Die Zuordnung der Identität des Arbeitsplatzes zu dem am Arbeitsplatz zur Verfügung stehenden eHealth-Kartenterminals mit deren Anzeige, PIN-Pad und den Chipkartenslots. Für die eHealth-Kartenterminals wird nach dem Aufstellungsort und dem Zugriff durch der Benutzer des Arbeitsplatzes unterschieden zwischen (a) den lokal am Arbeitsplatz aufgestellten eHealth-Kartenterminals, deren gesteckte Chipkarten er zugreifen, dessen PIN-Pad er bedienen und dessen Anzeige des Arbeitsplatzes er sehen kann, und (b) den entfernt vom Arbeitsplatz aufgestellten eHealth-Kartenterminals, auf deren gesteckte Chipkarten er remote zugreifen darf, ohne das PIN-Pad bedienen oder die Anzeige sehen zu können.
Kartenhandle	Daten zur Identifizierung einer gesteckten Chipkarte in einem konfigurierten eHealth-Kartenterminal.

Tabelle 14: Übersicht über TSF Daten

6.2. Funktionale Sicherheitsanforderungen des Netzkonnektors

Die funktionalen Sicherheitsanforderungen werden im Folgenden nicht wie sonst häufig in alphabetischer Reihenfolge aufgezählt, sondern nach funktionalen Gruppen gegliedert. Dadurch soll ein besseres Verständnis der Anforderungen und ihrer Abhängigkeiten untereinander erreicht werden. Die funktionalen Gruppen orientieren sich an den in Abschnitt 1.3.5 beschriebenen Sicherheitsdiensten (hier nur kurz in Stichworten rekapituliert):

- VPN-Client: gegenseitige Authentisierung, Vertraulichkeit, Datenintegrität, Informationsflusskontrolle (erzwungene VPN-Nutzung für sensitive Daten);
- Dynamischer Paketfilter: sowohl für WAN als auch für LAN;

- Netzdienste: Zeitsynchronisation über sicheren Kanal, Zertifikatsprüfung mittels Sperrlisten;
- Stateful Packet Inspection: Generierung von Audit-Daten für spätere zustandsgesteuerte Filterung;
- Selbstschutz: Speicheraufbereitung, Selbsttests, sicherer Schlüsselspeicher, Schutz von Geheimnissen, optional sichere Kanäle zu anderen Komponenten des Konnektors, Protokollierung Sicherheits-Log;
- Administration: Möglichkeit zur Wartung, erzwungene Authentisierung des Administrators, eingeschränkte Möglichkeit der Administration von Firewall-Regeln;
- Nutzung starker kryptographischer Verfahren für TLS-Verbindungen.

Um die Semantik von Sicherheitsanforderungen leichter erkennen zu können, wurden den Anforderungen teilweise **Suffixe** angehängt, z. B. „/NK.VPN_TI“ für den Trusted Channel, der den VPN-Kanal in die Telematikinfrastruktur fordert (siehe FTP_ITC.1/NK.VPN_TI). Diese Vorgehensweise erleichtert es auch, inhaltlich zusammenhängende Anforderungen zu identifizieren (z. B. FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF und FMT_MSA.3/NK.PF) und iterierte Komponenten zu unterscheiden. Für alle SFRs des Netzkonnektors aus diesem Kapitel wurde zudem das Suffix „NK“ verwendet, selbst wenn keine Iteration vorliegt.

6.2.1. VPN-Client

VPN

Der EVG stellt einen sicheren Kanal zur zentralen Telematikinfrastruktur-Plattform (TI-Plattform) sowie zum Sicheren Internet Service bereit, der nach gegenseitiger Authentisierung die Vertraulichkeit und Datenintegrität der Nutzdaten sicherstellt (vgl. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS).

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

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

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_TI The TSF shall provide a communication channel between itself and another trusted IT product **VPN-Konzentrator der Telematikinfrastruktur**[68] that is logically distinct from other communication channels and provides assured identification of its

68 refinement

end points **using certificate based authentication**[69] and protection of the channel data from modification **and**[70] disclosure.

FTP_ITC.1.2/NK.VPN_TI The TSF shall permit the TSF[71] 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*[72].

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 [76], RFC 4301 (IPsec) [48], RFC 4303 (ESP) [51]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [52]) unterstützt werden.

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

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

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

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

Dependencies: No dependencies.

FTP_ITC.1.1/NK.VPN_SIS The TSF shall provide a communication channel between itself and another trusted IT product **Sicherer Internet Service (SIS)**[73] that is logically distinct from other communication channels and provides assured identification of its end points **using**

69 refinement

70 refinement (or → and)

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

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

73 refinement

certificate based authentication[74] and protection of the channel data from modification **and**[75] disclosure.

FTP_ITC.1.2/NK.VPN_SIS The TSF shall permit the TSF[76] 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*[77].

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 [76], RFC 4301 (IPsec) [48], RFC 4303 (ESP) [51]). Zusätzlich soll **NAT-Traversal** (siehe RFC 7296 [52]) unterstützt werden.

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

Erläuterung: Die von O.NK.VPN_Auth geforderte gegenseitige Authentisierung der Endpunkte wird durch FTP_ITC.1.1/NK.VPN_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.

Anwendungshinweis 77: Der EVG muss RFC 7296 (IKEv2) [52] unterstützen, siehe [74], 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 Schutzprofil nicht behandelt. Falls ein Produkt eine solche Funktionalität bietet, darf sie die Sicherheit der Anwendungen gemäß § 291 a SGB V nicht beeinträchtigen.

Informationsflusskontrolle

Regelbasiert müssen alle schützenswerten Informationsflüsse die etablierten VPN-Tunnel nutzen. Nur Informationsflüsse, die vom Konnektor initiiert wurden sowie Informationsflüsse

74 refinement

75 refinement (or → and)

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

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

von Clientsystemen in Bestandsnetze dürfen den VPN-Tunnel in die Telematikinfrastruktur benutzen und erhalten damit überhaupt erst Zugriff auf die zentrale Telematikinfrastruktur-Plattform. Andere Informationsflüsse, die den Zugriff auf Internet-Dienste aus den lokalen Netzen der Leistungserbringer betreffen, müssen den VPN-Tunnel zum Sicheren Internet Service benutzen.

Diese Aspekte ergeben sich zwar aus der Betrachtung der VPN-Kanäle (aufgrund der Frage: Wie wird der Eingang in den VPN-Tunnel geschützt?), sie werden aber im Hinblick auf ihre Realisierung der Anforderung nach Informationsflusskontrolle mittels einem dynamischen Paketfilter (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF, siehe unten in Abschnitt 6.2.2) zugeordnet; das „PF“ steht dabei für Paketfilter. Daher finden sich die Anforderungen (SFR) zu diesen Aspekten im nächsten Abschnitt 6.2.2.

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

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

Dynamischer Paketfilter

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

FDP_IFC.1/NK.PF Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

hier erfüllt durch: FDP_IFF.1/NK.PF

FDP_IFC.1.1/ NK.PF The TSF shall enforce the *packet filtering SFP (PF SFP)*[78] on the *subjects*

(1) IAG,

(2) VPN concentrator of the TI,

(3) VPN concentrator of the SIS,

(4) the TI services ,

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

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

78 [assignment: *information flow control SFP*]

(7) active entity in the LAN,

(8) CRL download server,

(9) hash&URL server,

(10) registration server of the VPN network provider,

(11) remote management server,

the information

(1) incoming information flows

(2) outgoing information flows

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[79].

Anwendungshinweis 79: Die dynamischen Paketfilter (LAN-seitig und WAN-seitig) sollen sowohl den EVG vor Angriffen bzw. vor unerlaubten Informationsflüssen (i) aus dem LAN und (iii) aus dem WAN schützen als auch die Informationsflüsse zwischen (ii) LAN und WAN bzw. (iv) zwischen WAN und LAN kontrollieren.

Anwendungshinweis 80: Systembedingt bietet IPv4 (Internet Protocol, Version 4) nur eine Identifikation der Informationsflüsse, aber keine Authentisierung. Aus Mangel an besseren Mechanismen müssen dennoch auf dieser Basis die Entscheidungen über die Zulässigkeit von Informationsflüssen getroffen werden.

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

IP-Adressbereich	Instanz für Kommunikation mit dem Konnektor
ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der WAN-Adapter des Konnektors angeschlossen ist.
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske des lokalen Netzes des LE, in dem der LAN-Adapter des Konnektors angeschlossen ist.
ANLW_LEKTR_INTRANET_ROUTES	Adressbereich des Intranet-VPN des LE
NET_SIS	VPN-Konzentratoren der SIS
NET_TI_ZENTRAL	Zentrale Dienste der TI
NET_TI_DEZENTRAL	Adressbereich den WAN-Schnittstellen der Konnektoren für die Kommunikation mit der TI oder den Bestandsnetzen
NET_TI_OFFENE_FD	Offene Fachdienste der TI
NET_TI_GESICHERTE_FD	Gesicherte Fachdienste der TI

79 [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_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

IP-Adressen	Erläuterung
ANLW_LAN_IP_ADDRESS	LAN-seitige Adresse des EVG, unter dieser Adresse werden die Dienste des Konnektors im lokalen Netzwerk bereitgestellt werden.
ANLW_WAN_IP_ADDRESS	WAN-seitige Adresse des EVG
VPN_TUNNEL_TI_INNER_IP	IP-Adresse des Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren der TI
VPN_TUNNEL_SIS_INNER_IP	IP-Adresse des Konnektors als Endpunkt der IPSec-Kanäle mit den VPN-Konzentratoren des SIS
ANLW_IAG_ADDRESS	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.

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

Konfigurationsparameter	Bedeutung und [Werte]
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*[80] based on the following types of subject and information security attributes:

For all subjects and information as specified in FDP_IFC.1/NK.PF, the decision shall be based on the following security attributes:

(1) IP address,

(2) port number,

(3) protocol type,

(4) *direction (inbound and outbound IP*[81] *traffic)*

The subject active entity in the LAN has the security attribute IP address within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES[82]*.*

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,

80 [assignment: *information flow control SFP*]

81 IP = Internet Protocol

82 [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 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 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 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 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≠"").*

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

(1) *The TSF shall enforce SFP rules ANLW_FW_SIS_ADMIN_RULES*

(2) *The TSF shall transmit data (except for establishment of VPN connections) to the WAN only if the IPsec VPN tunnel between the TSF and the remote VPN concentrator has been successfully established and is active and working*[83].

FDP_IFF.1.4/NK.PF The TSF shall explicitly authorise an information flow based on the following rules*: Stateful Packet Inspection,* [assignment: *rules, based on security attributes, that explicitly authorise information flow*][84].

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.

(7) The TSF prevents communication of entities with IP addresses in the inner header within NET_TI_ZENTRAL,

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

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

NET_TI_GESICHERTE_FD, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE, ANLW_LAN_ADDRESS_SEGMENT, ANLW_LEKTR_INTRANET_ROUTES and ANLW_WAN_NETWORK_SEGMENT coming through the VPN tunnel with VPN concentrator of the SIS.

(8) The TSF prevents receive of packets from entities in LAN if packet destination is internet and (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS = KEINER).

(9) The TSF prevents inbound packets of the VPN channels from SIS with destination address in the inner header outside
a) ANLW_LAN_IP_ADDRESS or
b) ANLW_LEKTR_INTRANET_ROUTES if ANLW_WAN_ADAPTER_MODUS=DISABLED or
c) ANLW_WAN_IP_ADDRESS if ANLW_WAN_ADAPTER_MODUS=ACTIVE

(10) The TSF prevents communication of IAG to connector through LAN interface if (ANLW_WAN_ADAPTER_MODUS= ACTIVE).

(11) The TSF prevents communication of IAG to connector through WAN interface of the connector if (ANLW_WAN_ADAPTER_MODUS= DISABLED).

(12) [*assignment*: *additional rules, based on security attributes, that explicitly deny information flows*][85].

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

Erläuterung: Der von O.NK.PF_WAN und O.NK.PF_LAN geforderte dynamische Paketfilter wird durch FDP_IFC.1/NK.PF und FDP_IFF.1/NK.PF gefordert.

Anwendungshinweis 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 6.4.2) 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: Dazu muss der EVG Informationen über eine (kurze) Historie der Verbindung verwalten. Beispielsweise werden eingehende Verbindungen nur als Antworten auf zuvor ausgegangene Anfragen zugelassen, so dass ein ungefragter Verbindungsaufbau aus dem WAN wirkungsvoll verhindert wird. Siehe auch stateful packet inspection im Glossar.

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

Anwendungshinweis 83: Die dynamische Paketfilterung soll die Menge der **zulässigen Protokolle** im Rahmen der Kommunikation mit der Telematikinfrastruktur geeignet beschränken. Der ST-Autor muss die zulässigen Protokolle gemäß Spezifikation Konnektor [gemSpec_Kon] [76] und Spezifikation Netzwerk [gemSpec_Net] [89] benennen. Der EVG beschränkt den freien Zugang zum als unsicher angesehenen Transportnetz (WAN) geeignet zum Schutz der Clientsysteme.

Der ST-Autor kann mittels FDP_IFF.1.3/NK.PF bis FDP_IFF.1.5/NK.PF weitere Regeln ergänzen, die der EVG umsetzt. Mindestens sollen die Anforderungen an die in O.NK.PF_LAN beschriebene **Informationsflusskontrolle** an dieser Stelle formuliert werden (EVG erzwingt, dass *zu schützende Daten der TI und der Bestandsnetze* und *zu schützende Nutzerdaten* über den VPN-Tunnel in die Telematikinfrastruktur bzw. zum Internet versendet werden; EVG verhindert ungeschützten Zugriff auf das Transportnetz). Darüber hinaus können weitere Regeln ergänzt werden, etwa weitere Plausibilitätskontrollen; dies ist aber nicht zwingend erforderlich: Bei einem assignment ist auch die Auswahl von *none* zulässig.

Die von FDP_IFF.1.2/NK.PF geforderten Filterregeln (packet filtering rules) sind mit geeigneten Default-Werten vorbelegt (siehe unten, FMT_MSA.3/NK.PF) und können vom Administrator verwaltet werden (siehe FMT_MSA.1/NK.PF, vgl. Abschnitt 6.2.6 Administration).

FMT_MSA.3/NK.PF Static attribute initialisation

Restriktive Paketfilter-Regeln

Dependencies: FMT_MSA.1 Management of security attributes

hier erfüllt durch: FMT_MSA.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_MSA.3.1/NK.PF The TSF shall enforce the *PF SFP*[86] to provide restrictive[87] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Refinement: Bei den Sicherheitsattributen handelt es sich um die Filterregeln für den dynamischen Paketfilter (FDP_IFF.1.2/NK.PF). *Restriktive* bedeutet, dass Verbindungen, die nicht ausdrücklich erlaubt sind, automatisch verboten sind. Außerdem muss der EVG bei Auslieferung mit einem Regelsatz ausgeliefert werden, der bereits einen grundlegenden Schutz bietet.

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

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

Anwendungshinweis 84: In FMT_MSA.3.2/PF soll der ST-Autor spezifizieren, welche administrativen Rollen alternative Default-Werte spezifizieren dürfen. Denkbar ist insbesondere der lokale Administrator (siehe auch FMT_SMR.1./NK). Das Security Target kann aber auch ein feineres Rollenmodell spezifizieren.

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

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

6.2.3. Netzdienste

Zeitsynchronisation

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

FPT_STM.1/NK Reliable time stamps

Der EVG stellt verlässliche Zeitstempel bereit, indem er die Echtzeituhr gemäß OE.NK.Echtzeituhr regelmäßig synchronisiert.

Dependencies: No dependencies.

FPT_STM.1.1/NK The TSF shall be able to provide reliable time stamps.

Refinement: Die Zuverlässigkeit (*reliable*) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [47] erreicht.

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

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

Anwendungshinweis 85: Zum Zeitdienst siehe Konnektor-Spezifikation [76], Abschnitt 4.2.5 *Zeitdienst.*

Anwendungshinweis 86: Der ST-Autor soll das Refinement verschärfen, falls die aktuelle Version der Konnektor-Spezifikation [76] eine häufigere Zeitsynchronisation fordert als im Refinement zu FPT_STM.1/NK (einmal innerhalb von 24 Stunden) gefordert. Die Anforderung aus dem Refinement zu FPT_STM.1/NK bleibt in jedem Fall Mindestanforderung, auch für den Fall, dass die Konnektor-Spezifikation weniger strenge Anforderungen formulieren sollte.

Anwendungshinweis 87: Gemäß Konnektor-Spezifikation [76], Abschnitt 3.3 *Betriebszustand*, erfolgen Hinweise an den Administrator über kritische Betriebszustände des Konnektors. Darüber hinaus fordert [76]

- *Im Betrieb MUSS der Zustand des Konnektors erkennbar sein. Zur Anzeige des Betriebszustandes des Konnektors SOLL es eine Signaleinrichtung am Konnektor geben***.** [TIP1-A_4843].

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

Da sich die logische Clientsystem-Schnittstelle im AK (und nicht im NK) befindet, wurde die Anforderung FPT_FLS.1 dem Anwendungskonnektor zugeordnet.

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

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

Zertifikatsprüfung

Der EVG muss die Gültigkeit der Zertifikate überprüfen, die für den Aufbau der VPN-Kanäle verwendet werden. Die erforderlichen Informationen zur Prüfung der Gerätezertifikate werden dem EVG in Form einer (signierten) Trust-service Status List (TSL) und einer Sperrliste (CRL) bereitgestellt. Der EVG prüft die Zertifikate kryptographisch mittels der aktuell gültigen TSL und CRL.

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

Prüfung der Gültigkeit von Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.Zert The TSF shall provide the capability to consistently interpret *information – distributed in the form of a TSL (Trust-Service Status List) and CRL (Certificate Revocation List) information – about the validity of certificates and about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects*[88] when shared between the TSF and another trusted IT product.

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

FPT_TDC.1.2/NK.Zert The TSF shall use *interpretation rules*[89] when interpreting the TSF data from another trusted IT product.

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

Anwendungshinweis 88: Der ST-Autor soll die *interpretation rules* in FPT_TDC.1.2/NK.Zert geeignet verfeinern; dazu soll er sich an der aktuellen Version der Konnektor-Spezifikation [76] orientieren.

Anwendungshinweis 89: Die TSL und die CRL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [76] 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 [76]).

6.2.4. Stateful Packet Inspection

Der EVG kann nicht wohlgeformte IP-Pakete erkennen und verwirft diese. Er implementiert eine sogenannte „zustandsgesteuerte Filterung“ (engl. „stateful packet inspection“ oder auch „stateful inspection“ genannt). Dies ist eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer aktiven Session zugeordnet und der Verbindungsstatus in die Entscheidung über die Zulässigkeit eines Informationsflusses einbezogen wird. Siehe auch Anwendungshinweis 16.

Anwendungshinweis 90: Weitergehende Angriffe gegen die Systemintegrität des EVG müssen abgewehrt werden (robuste Implementierung, Resistenz gegen Angriffe wie von AVA_VAN.3 gefordert), aber nicht im Detail erkannt werden (es wird keine komplexe Erkennungslogik für Angriffe gefordert).

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

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

6.2.5. Selbstschutz

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

Speicheraufbereitung

Der EVG löscht nicht mehr benötigte kryptographische Schlüssel (insbesondere session keys für die VPN-Verbindung) nach ihrer Verwendung durch aktives Überschreiben (FDP_RIP.1/NK). Der EVG speichert medizinische Daten nicht dauerhaft. Ausnahmen sind

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

die Speicherung von Daten während ihrer Ver- und Entschlüsselung; auch diese werden sobald wie möglich nach ihrer Verwendung gelöscht.

FDP_RIP.1/NK Subset residual information protection

	Speicheraufbereitung (Löschen nicht mehr benötigter Schlüssel direkt nach ihrer Verwendung durch aktives Überschreiben); keine dauerhafte Speicherung medizinischer Daten.
Dependencies:	No dependencies.
FDP_RIP.1.1/NK	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[90] the following objects: *cryptographic keys (and session keys) used for the VPN or for TLS-connections, user data (zu schützende Daten der TI und der Bestandsnetze and zu schützende Nutzerdaten),* [assignment: *list of objects*][91].
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: Wann Daten nicht mehr benötigt werden und somit aktiv überschrieben werden müssen, soll sinnvoll festgelegt werden; dabei sollten weitere Aspekte wie Performance und Vermeidung unnötig häufiger Schlüsselableitungen berücksichtigt werden. Der Konnektor speichert *zu schützende Daten der TI und der Bestandsnetze* oder *zu schützende Nutzerdaten* niemals dauerhaft; er speichert sie lediglich temporär zur Verarbeitung (z. B. während einer Ver- oder Entschlüsselung). Das offene Assigment des Elements FDP_RIP.1.1/NK darf leer sein

Selbsttests

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

FPT_TST.1/NK TSF testing

	Selbsttests
Dependencies:	No dependencies.
FPT_TST.1.1/NK	The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[92].

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

91 [assignment: *list of objects*]

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

FPT_TST.1.3/NK The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*] .

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

- die Prüfung kryptographischer Verfahren bei Programmstart,
- 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: Beispiele für die im Refinement geforderten Mechanismen sind:

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

Schutz von Geheimnissen, Seitenkanalresistenz

Der EVG schützt Geheimnisse während ihrer Verarbeitung gegen unbefugte Kenntnisnahme einschließlich der Kenntnisnahme nach Angriffen durch Seitenkanal-Analysen (side channel analysis). Dies gilt grundsätzlich für *kryptographisches Schlüsselmaterial* (siehe Tabelle 2: Sekundäre Werte in Abschnitt 3.1.1.1). Zur Definition der Anforderung FPT_EMS.1/NK siehe Abschnitt 5.1.

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

FPT_EMS.1/NK Emanation of TSF and User data

Dependencies: No dependencies.

FPT_EMS.1.1/NK The TOE shall not emit *sensitive data (as listed below) – or information which can be used to recover such sensitive data – through network interfaces (LAN or WAN)*[93] in excess of *limits that ensure that no leakage of this sensitive data occurs*[94] enabling access to

93 [assignment: *types of emissions*]

94 [assignment: *specified limits*]

- *session keys derived in course of the Diffie-Hellman-Keyexchange-Protocol,*
- *[selection: none, key material used to verify the TOE's integrity during self tests],*
- *[selection: none, key material used to verify the integrity and authenticity of software updates],*
- *[selection: none, key material used to decrypt encrypted software updates (if applicable)],*
- *[selection: none, key material used for authentication of administrative users (if applicable)],*
- *[assignment: list of other types of TSF data (may be empty)]*[95] and
- *data to be protected ("*zu schützende Daten der TI und der Bestandsnetze")
- *[assignment: list of types of user data (may be empty)]*[96].

FPT_EMS.1.2/NK The TSF shall ensure *attackers on the transport network (WAN) or on the local network (LAN)*[97] are unable to use the following interface *WAN interface or LAN interface of the connector*[98] to gain access to **the sensitive data (TSF data and user data) listed above**[99].

Anwendungshinweis 93: Der ST-Autor kann hier weitere Verfeinerungen vornehmen. Siehe auch Abschnitt 7.6.16 von [69].

Sicherheits-Log

Der EVG führt ein Sicherheits-Log wie unter Sicherheitsdienst *Protokollierung* in Abschnitt 1.3.5.1 beschrieben. Vergleiche dazu auch die Konnektor-Spezifikation [76], Abschnitt 4.1.10.

FAU_GEN.1/NK.SecLog Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

hier erfüllt durch: FPT_STM.1/NK

FAU_GEN.1.1/NK.SecLog The TSF shall be able to generate an audit record of the following auditable events:

---

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

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

97 [assignment: *type of users*]

98 [assignment: *type of connection*]

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

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c)

- *start-up, shut down and reset (if applicable) of the TOE*
- *VPN connection to TI successfully / not successfully established,*
- *VPN connection to SIS successfully / not successfully established,*
- *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.*[100]

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

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

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

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

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

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

Anwendungshinweis 94: Der ST-Autor soll die Liste in FAU_GEN.1.1/NK.SecLog, Punkt c) in Abstimmung mit der Zertifizierungsstelle und der Konnektor-Spezifikation [76] (Abschnitte 3.2 und 3.3, Tabelle 3) abgleichen. Die Konnektor-Spezifikation fordert die Initialisierung des Protokollierungsdienstes und weiterer Dienste in der Boot-Phase und die Meldung des Abschlusses der Boot-Phase durch den Event "BOOTUP/ BOOTUP_COMPLETE". Wenn der Protokollierungsdienst als erster Dienst gestartet wird, so kann dieser Zeitpunkt als Zeitpunkt für das Ereignis „start-up“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet werden. Wenn der Protokollierungsdienst als letzter Dienst bei einem Shut-down des EVG beendet wird, so kann dieser Zeitpunkt als Zeitpunkt für das Ereignis „*shut down*“ in FAU_GEN.1.1/NK.SecLog, Punkt c) verwendet werden.

Anwendungshinweis 95: Die exakte Größe des für das Security Log zu reservierenden Speicherbereichs ist somit abhängig von der Größe der einzelnen Log-Einträge, von der verwendeten Kodierung (z. B.: Ereignismeldung im Klartext als ASCII-kodierter String der Länge 80 Zeichen vs. Kodierung des Ereignistyps als Nummer in einem Byte) und weiteren Produkteigenschaften, beispielsweise vom eventuellen Vorhandensein optionaler Auswertelogik, welche bewusste Verdrängungsversuche während der Protokollierung erkennt und verhindert. Stößt ein Angreifer beispielsweise wiederholt dieselbe Aktion an, die zu einem Log-Eintrag führt, könnte der EVG nach einer gewissen Anzahl dazu übergehen, nur noch die Anzahl der Ereignisse zu zählen und nicht für jedes Ereignis einen vollständigen Log-Eintrag zu schreiben. Dabei muss jedoch sichergestellt sein, dass die geforderten Informationen weiterhin verfügbar sind. Beispiel: Es gab 1846 fehlgeschlagene Login-Versuche als Administrator, davon die ersten zehn zu folgenden Zeiten (Datum und Uhrzeit), die letzten 50 zu folgenden Zeiten (Datum und Uhrzeit) und die übrigen in regelmäßigen Abständen (oder: gehäuft immer gegen Mitternacht).

FAU_GEN.2/NK.SecLog User identity association

Dependencies: FAU_GEN.1 Audit data generation

hier erfüllt durch: FAU_GEN.1/NK.SecLog

FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

FAU_GEN.2.1/NK.SecLog For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Anwendungshinweis 96: Der EVG muss bei Konfigurationsänderungen durch authentisierte Administratoren die Identität des ändernden Administrators in das Sicherheits-Log aufnehmen. Falls der EVG mehrere Administrator-Rollen unterstützt, soll der Sicherheits-Log-Eintrag die jeweilige Administrator-Rolle eindeutig identifizieren.

6.2.6. Administration

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

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

Anwendungshinweis 63. In diesem Schutzprofil wird davon ausgegangen, dass der AK die Authentisierung für den EVG durchführt.

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

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

FMT_SMR.1./NK Security roles

Dependencies: FIA_UID.1 Timing of identification

hier erfüllt durch: FIA_UID.1/NK.SMR

FMT_SMR.1.1/NK The TSF shall maintain the roles

- *Administrator*,
- *SIS*,
- *TI*
- *Anwendungskonnektor*[101].

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

FMT_MTD.1/NK Management of TSF data

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

FMT_MTD.1.1/NK The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clear*, [assignment: *other operations*]] the

101 [assignment: *the authorised identified roles*]

real time clock, packet filtering rules [assignment: list of other TSF data (may be empty)][102] to *the role Administrator*[103].

Refinement: Die *real time clock* bezieht sich auf die von OE.NK.Echtzeituhr geforderte Echtzeituhr. Obwohl die Echtzeituhr in der Umgebung liegt, wird ihre Zeit vom EVG genutzt und der EVG beschränkt den Zugriff (*modify* = Einstellen der Uhrzeit) auf diese Echtzeituhr. Die *packet filtering rules* legen das Verhalten des Paketfilters (O.NK.PF_LAN, O.NK.PF_WAN) fest.

Anwendungshinweis 99: Nur Administratoren dürfen administrieren: Die aufgelisteten administrativen Tätigkeiten können nur von Administratoren ausgeführt werden.

Anwendungshinweis 100: Falls der EVG ein **Deaktivieren der VPN-Verbindung** erlaubt, darf nur der Administrator dieses Deaktivieren vornehmen. Dazu soll der ST-Autor die Managementfunktion „Aktivieren und Deaktivieren des VPN-Tunnels“ in die Liste bei FMT_SMF.1/NK aufnehmen und innerhalb von FMT_MTD.1/NK den Zugriff auf diese Managementfunktion auf den Administrator beschränken.

FIA_UID.1/NK.SMR Timing of identification

Identification of Security Management Roles

Dependencies: No dependencies.

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

- *all actions except for administrative actions (as specified by FMT_SMF.1*/NK*, see below)*[104]

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

FTP_TRP.1/NK.Admin Trusted path

Trusted Path für den Administrator.

Dependencies: No dependencies.

FTP_TRP.1.1/NK.Admin The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct

102 [assignment: *list of TSF data*]

103 [assignment: *the authorised identified roles*]

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

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

FTP_TRP.1.2/NK.Admin The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3/NK.Admin The TSF shall require the use of the trusted path for *initial user authentication and administrative actions*.[105]

Anwendungshinweis 102: Der ST-Autor kann sich durch die Selection remote / local aussuchen, ob die Wartung über die LAN-Schnittstelle (PS1) und/oder über die WAN-Schnittstelle (PS2) erfolgen kann. Abhängig davon, wie der EVG gewartet werden kann, soll der ST-Autor die Selection vornehmen.

FMT_SMF.1/NK Specification of Management Functions

Dependencies: No dependencies.

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

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)

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

  (Verwalten der TLS-Verbindungen durch den Anwendungskonnektor.) [106]

Anwendungshinweis 103: Optional kann der EVG auch das Review (Lesen und Auswerten) der von FAU_GEN.1/NK.SecLog erzeugten Audit-Daten als Managementfunktion anbieten.

FMT_MSA.1/NK.PF Management of security attributes

Nur der Administrator darf (gewisse) Filterregeln verändern.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

FMT_SMR.1 Security roles

hier erfüllt durch: FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch: FMT_SMF.1/NK

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

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

FMT_MSA.1.1/NK.PF The TSF shall enforce the *PF SFP*[107] to restrict the ability to *[selection: query, modify, delete, [assignment: other operations]]*[108] the security attributes *packet filtering rules*[109] to *the roles „Administrator“, [assignment (may be empty): other authorised identified roles]*[110].

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 [76], Kapitel 4.2.1.1, Parameter MGM_LU_ONLINE). Der Administrator darf zusätzlich einschränkende Regeln für die Kommunikation mit dem SIS festlegen (siehe Konnektorspezifikation [76], Kapitel 4.2.1.2, ANLW_FW_SIS_ADMIN_RULES) festlegen. Vorgabewerte dürfen nicht verändert werden („change-default“ ist nicht erlaubt).

Erläuterung: FMT_MSA.1/NK.PF sorgt als von FMT_MSA.3/NK.PF abhängige Komponente dafür, dass die Regeln für den Paketfilter (*packet filtering rules*, diese Regeln werden als security attributes angesehen) nur durch den Administrator oder eine andere kompetente Instanz (siehe FMT_SMR.1./NK) verändert werden können. Weiterhin legt die Konnektorspezifikation [76] 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

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

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

109 [assignment: *list of security attributes*]

110 [assignment: *the authorised identified roles*]

dem Transportnetz bzw. der Telematikinfrastruktur oder auch die Kommunikation zwischen dem LAN und dem Transportnetz bzw. der Telematikinfrastruktur betreffen, nicht durch einen administrativen Eingriff (Konfiguration) des Administrators außer Kraft gesetzt werden können.

Anwendungshinweis 104: Zu den verschiedenen laut Konnektor-Spezifikation zulässigen Optionen der Administration von Firewall-Regeln gelten die in Kapitel 4.2.1 [76] definierten Anforderungen.

Anwendungshinweis 105: Eine Möglichkeit, Firewall-Regeln zu aktualisieren, besteht darin, ein **Software-Update** einzuspielen (grundsätzlich im Rahmen der Auslieferung einer neuen Version des EVGs – oder aber als zusätzliche, optionale Funktionalität des EVGs; siehe unten).

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

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

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

Anwendungshinweis 106: Das Schutzprofil verbietet es nicht, dass der Netzkonnektor seine Filterregeln abhängig von Ereignissen anderer Konnektorteile (z. B. Anwendungskonnektor) dynamisch anpasst (Beispiel: Operation *subscribe* beim cetp-Protokoll).

FMT_MSA.4/NK Security attribute value inheritance

Definition von Regeln für die Sicherheitsattribute

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

hier erfüllt durch: FDP_IFC.1/NK.PF

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

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

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

Wenn die Authentisierung des Administrators in der IT-Einsatzumgebung erfolgt und nicht erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diesen Status und weisen

*dem Sicherheitsattribut „Autorisierungsstatus“ des auf diese Weise nicht authentisierten Benutzers „Administrator“ den Wert „**nicht autorisiert**“ zu.*[111]

Subjekt	Sicherheitsattribut	Mögliche Werte
Administrator	Autorisierungsstatus	autorisiert, nicht autorisiert

Anwendungshinweis 107: Mit *IT-Einsatzumgebung* sind hier die anderen Konnektorteile, wie der Anwendungskonnektor gemeint. In diesem Schutzprofil wird davon ausgegangen, dass der AK die Authentisierung für den EVG durchführt. Siehe auch OE.NK.Admin_Auth und Anwendungshinweis 63.

6.2.7. Kryptographische Basisdienste

Der Konnektor soll laut Dokument „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt]“ [74] die im Folgenden aufgelisteten kryptographischen Primitive implementieren.

Anwendungshinweis 108: Die SFR der Familie FCS in CC Teil 2 [2] enthalten ein [assignment: *cryptographic algorithm*]. Diese Zuweisungen wurden in den SFR dieses Kapitels in Übereinstimmung mit den gematik-Spezifikationen und Technischen Richtlinien des BSI vorgenommen. Die TSF muss die darüberhinausgehenden verpflichtenden Vorgaben der angegebenen Standards soweit sie die angegebenen Algorithmen und Protokollen betreffen implementieren und darf den angegebenen Standards mit Ausnahme der zugewiesenen Kryptoalgorithmen nicht widersprechen. So fordert RFC 3602 die Unterstützung von AES 128 Bit, die Zuweisung des SFR FCS_COP.1/NK.ESP aber in Übereinstimmung mit der Spezifikation kryptographischer Algorithmen in der Telematikinfrastruktur [74] an seiner Stelle verbindlich den stärkeren AES 256 Bit. Die Zuweisung erfordert nicht, dass die TSF alle in den angegeben Standards zulässigen Optionen für die spezifizierten kryptographischen Operationen und Schlüsselmanagementfunktionen implementieren muss. Die Anforderungen an die Gewährleistung der Interoperabilität sind hiervon nicht betroffen.

Anwendungshinweis 109: Die Implementierung des Blockchiffre Advanced Encryption Standard (AES) ist eine für den TOE sicherheitsrelevante Funktionalität. Bezüglich der Zulässigkeit der Nutzung einer zusätzlichen im Rahmen der Evaluierung nach diesem PP nicht untersuchten AES-Implementierung gelten die Aussagen der Technischen Richtlinie BSI TR-03116-1 [68]. In jedem Fall muss der TOE stets den Wechsel zur geprüften AES-Implementierung durch den Administrator ermöglichen und diese als Voreinstellung vorsehen. Die korrekte Funktion des Wechsels ist im Rahmen der Evaluierung zu dokumentieren.

FCS_COP.1/NK.Hash Cryptographic operation

Zu unterstützende Hash-Algorithmen

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

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

FCS_CKM.4 Cryptographic key destruction

Alle bisher für FCS_COP.1/NK.Hash genannten Abhängigkeiten werden nicht erfüllt. Begründung: Bei einem Hash-Algorithmus handelt es sich um einen kryptographischen Algorithmus, der keine kryptographischen Schlüssel verwendet. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels und zu seiner Zerstörung erforderlich.

FCS_COP.1.1/NK.Hash The TSF shall perform *hash value calculation*[112] in accordance with a specified cryptographic algorithm *SHA-1, SHA-256, [assignment: list of SHA-2 Algorithms with more than 256 bit size]*[113] and cryptographic key sizes *none*[114] that meet the following: *FIPS PUB 180-4 [14]*.[115]

FCS_COP.1/NK.HMAC Cryptographic operation

Zu unterstützende Hash basierende MAC-Algorithmen

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.HMAC The TSF shall perform *HMAC value generation and verification*[116] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, [assignment: list of SHA-2 Algorithms with 256bit size or more]*[117] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *FIPS PUB 180-4 [14], RFC 2404 [55], RFC 4868 [56], RFC 7296 [52]*.[118]

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

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

[113] [assignment: *cryptographic algorithm*]

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

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

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

[117] [assignment: *cryptographic algorithm*]

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

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 erüllt.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.

FCS_COP.1.1/NK.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K storing the signing key and performing the RSA operation* [119]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[120] and cryptographic key sizes *2048 bit*[121] that meet the following: *RFC 8017 (PKCS#1) [31], FIPS PUB 180-4 [14]*[122].

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

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

[120] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1.1/NK.ESP The TSF shall perform *symmetric encryption and decryption with Encapsulating Security Payload*[123] in accordance with a specified cryptographic algorithm *AES-CBC (OID 2.16.840.1.101.3.4.1.42)*[124] and cryptographic key sizes *256 bit*[125] that meet the following: *FIPS 197 [15], RFC 3602 [54], RFC 4303 (ESP) [51],], specification [74]* [126].

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*[127] in accordance with a specified cryptographic algorithm *IPsec-protocol*[128] and cryptographic key sizes *256 bit*[129] that meet the following: *RFC 4301 (IPsec) [48], specification [74]*[130].

FCS_CKM.1/NK Cryptographic key generation

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

hier erfüllt durch: FCS_CKM.2/NK.IKE, FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec und FCS_COP.1/NK.Hash

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:

123 [assignment: *list of cryptographic operations*]

124 [assignment: *cryptographic algorithm*]

125 [assignment: *cryptographic key sizes*]

126 [assignment: *list of standards*]

127 [assignment: *list of cryptographic operations*]

128 [assignment: *cryptographic algorithm*]

129 [assignment: *cryptographic key sizes*]

130 [assignment: *list of standards*]

cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: *specification [74], TR-03116 [68]*[131].

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 Schutzprofil wurde eine Schlüsselgenerierung gewählt (siehe FCS_CKM.1/NK), da der EVG im Rahmen des Diffie-Hellman-Keyexchange-Protocols seine Sitzungsschlüssel (*session keys*) für die VPN-Kanäle ableitet; diese Ableitung wird als Schlüsselgenerierung angesehen. (Der Aspekt des Schlüsselaustausches mit einem VPN-Konzentrator wird als FCS_CKM.2/NK.IKE modelliert, siehe unten). Alle erzeugten Schlüssel müssen mindestens 100 bit Entropie besitzen, damit der Netzkonnektor resistent gegen Angriffe mit dem im Schutzprofil des Netzkonnektors ([69]) unterstellten hohen Angriffspotential sein kann.

FCS_CKM.2/NK.IKE Cryptographic key distribution

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.2.1/NK.IKE The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *IPsec IKE v2*[132] that meets the following *standard: RFC 7296 [52], specifications [74], TR-02102-3 [65]*[133].

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

131 [assignment: *list of standards*]

132 [assignment: *cryptographic key distribution method*]

133 [assignment: *list of standards*]

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

Anwendungshinweis 111: FCS_CKM.4/NK zerstört die von den Komponenten FCS_COP.1/... sowie FCS_CKM.2 (FCS_COP.1/NK.Auth, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE) benötigten Schlüssel. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle verwendeten Schlüssel. Der ST-Autor soll spezifizieren, wie die Schlüssel zerstört werden. Das Überschreiben der Schlüssel mit festen oder zufälligen Werten kann ein zulässiges Verfahren darstellen.

Anwendungshinweis 112: Der ST-Autor soll eventuelle Verfeinerungen der Zuweisungen der Operationen im Einklang mit den in Dokumenten [68], [74] und [76] vornehmen. Dieser Hinweis gilt für alle genannten SFRs FCS_COP.1/* sowie FCS_CKM.1/NK, FCS_CKM.2/NK.IKE und FCS_CKM.4/NK. Gleiches gilt für die in Kapitel 6.2.8 für TLS-Kanäle definierten Kryptoverfahren.

Der DH-Exponent für den Schlüsselaustausch soll eine Mindestlänge gemäß [74] aufweisen. Für IKE-Lifetime, IPsec-SA-Lifetime und Forward Secrecy sind die Vorgaben aus [74] zu beachten.

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

Die folgenden SFRs modellieren den TLS-Basisdienst und den Import bzw. Export von Zertifikaten. Tatsächlich verwendet werden die von der Spezifikation geforderten TLS-Verbindungen im Anwendungskonnektor.

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

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

Grundlegende Sicherheitsleistungen eines TLS-Kanals

Dependencies: No dependencies.

FTP_ITC.1.1/NK.TLS The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and **is able to**[134] provide**s** assured identification of its end points and protection of the channel data from modification **and**[135] disclosure.

134 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.

135 refinement (or → and)

FTP_ITC.1.2/NK.TLS The TSF **must be able to**[136] permit *the TSF or another trusted IT-Product*[137] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.TLS The TSF shall initiate communication via the trusted channel for *communication required by the Anwendungskonnektor, [assignment: list of other functions for which a trusted channel is required]*[138].

Refinement: Die Anforderung „protection of the channel data from modification **and** disclosure“ ist zu verstehen als Schutz der Integrität und der Vertraulichkeit (der Kanal muss beides leisten). Dabei umfasst hier „integrity“ außer der Verhinderung unbefugter Modifikation auch Verhinderung von unbefugtem Löschen, Einfügen oder Wiedereinspielen von Daten während der Kommunikation. Der Trusted Channel muss auf Basis des TLS-Protokolls aufgebaut werden (siehe Konnektor-Spezifikation [76] und [74], wobei TLS 1.2 gemäß RFC 5246 [58] unterstützt werden muss. Die folgenden Cipher Suiten MÜSSEN unterstützt werden:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,

TLS_DHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Die Anforderung „assured identification” im ersten Element des SFR impliziert, dass der EVG in der Lage sein muss, die Authentizität des „trusted IT-product“ zu prüfen. Im Rahmen dieser Überprüfung muss er in der Lage sein, eine Zertifikatsprüfung durchführen (siehe FPT_TDC.1/NK.TLS.Zert). Da allerdings der Anwendungskonnektor in Abhängigkeit von der TLS-Verbindung ggf. entscheiden kann, auf eine 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.

136 refinement (shall → must be able to)

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

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

Anwendungshinweis 113: Der EVG muss TLS Version 1.2 [58] unterstützen und kann zusätzlich TLS Version 1.3 [32] unterstützen (s. [74]). Der EVG muss alle im Refinement des SFRs genannten Kryptosuiten als Algorithmen für TLS unterstützen, dabei müssen die Anforderungen aus [74] erfüllt werden. Die Kryptosuiten sollen für die TLS-Kommunikation zwischen dem Anwendungskonnektor und anderen Komponenten genutzt werden. Der Konnektor darf TLS Version 1.0 und 1.1 sowie SSL nicht unterstützen.

FPT_TDC.1/NK.TLS.Zert Inter-TSF basic TSF data consistency

Prüfung der Gültigkeit von TLS-Zertifikaten

Dependencies: No dependencies.

FPT_TDC.1.1/NK.TLS.Zert The TSF shall provide the capability to consistently interpret

(1)X.509-Zertifikate für TLS-Verbindungen

(2)eine Liste gültiger CA-Zertifikate (Trust-Service Status List TSL)

(3)Sperrinformationen zu Zertifikaten für TLS-Verbindungen, die via OCSP erhalten werden

(4)importierte X.509 Zertifikate für Clientsysteme

(5)eine im Konnektor geführte Whitelist von Zertifikaten für TLS-verbindungen

(6)[assignment: additional list of data types][139]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS.Zert The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*][140] when interpreting the TSF data from another trusted IT product.

Refinement: Die „interpretation rules“ umfassen: Der EVG muss prüfen können, ob die Gültigkeitsdauer eines Zertifikates überschritten ist und ob ein Zertifikat in einer Whitelist oder in einer gültigen Zertifikatskette bis zu einer zulässigen CA (Letzteres ggf. anhand der TSL) enthalten ist. Ebenso muss sie anhand einer OCSP-Anfrage prüfen können, ob das Zertifikat noch gültig ist.

Anwendungshinweis 114: Der ST-Autor soll gegebenenfalls die *interpretation rules* geeignet verfeinern; dazu soll er sich an der aktuellen Version der Konnektor-Spezifikation [76] orientieren.

Anwendungshinweis 115: Die TSL muss gemäß Anforderung TIP1-A_4684 in der Konnektor-Spezifikation [76] 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 [76]).

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

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

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

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

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

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*[141] 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*[142] that meet the following: *Standard RFC 5246 [58]*.[143]

Anwendungshinweis 116: Der EVG muss TLS Version 1.2 [58] unterstützen und kann Version 1.3 [32] unterstützen (s. [74]). Wird TLS 1.3 unterstützt muss der Autor des ST die SFR FCS_CKM.1/NK.TLS um den entsprechenden Standard erweitern. Der EVG muss alle im SFR genannten cipher suites als Algorithmen für TLS unterstützen. Die Schlüsselerzeugung basiert auf dem Diffie-Hellman-Keyexchange-Protocol mit RSA-Signaturen (DHE_RSA nach [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 sollen für die TLS-Kommunikation zwischen dem EVG und anderen Komponenten genutzt werden. Es werden jeweils getrennte Schlüssel für jede Verwendung und Verschlüsselung nach FCS_COP.1/NK.TLS.AES und FCS_COP.1/NK.TLS.HMAC berechnet. Der EVG muss Schlüssel mit einer Entropie von mindestens 100 Bit erzeugen (siehe [68]). Bezüglich Diffie-Hellman-Gruppen für die Schlüsselaushandlung sind die Vorgaben aus [74] zu beachten. Der DH-Exponent für den Schlüsselaustausch soll eine Mindestlänge gemäß [74] aufweisen. Bezüglich Elliptic-Curve-Diffie-Hellman-Keyexchange müssen die gemäß [74] vorgegebenen Kurven unterstützt werden.

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

Zu unterstützende Hash basierende MAC-Algorithmen

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

141 [assignment: *cryptographic key generation algorithm*]

142 [assignment: *cryptographic key sizes*]

143 [assignment: *list of standards*]

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*[144] in accordance with a specified cryptographic algorithm *HMAC with SHA-1, SHA-256 and SHA-384*[145] and cryptographic key sizes *160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384*[146] that meet the following: *Standards FIPS 180-4 [14] and RFC 2104 [18]* [147].

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

FCS_COP.1/NK.TLS.AES Cryptographic operation

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

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

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

FCS_CKM.1 Cryptographic key generation]

hier erfüllt durch: FCS_CKM.1/NK.TLS

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_COP.1.1/NK.TLS.AES The TSF shall perform *symmetric encryption and decryption*[148] in accordance with a specified cryptographic algorithm *AES-128 and AES-256 in CBC and GCM Mode*[149] and cryptographic key sizes *128 bit for AES-128 and 256 bit for AES-256*[150] that meet the following: *FIPS 197 [15], NIST 800-38D [59],*

144 [assignment: *list of cryptographic operations*]

145 [assignment: *cryptographic algorithm*]

146 [assignment: *cryptographic key sizes*]

147 [assignment: *list of standards*]

148 [assignment: *list of cryptographic operations*]

149 [assignment: *cryptographic algorithm*]

150 [assignment: *cryptographic key sizes*]

RFC5246 [58], RFC 8422 [60], RFC 5289 [61], specification [74] [151].

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/NK.TLS.

Die *signature creation* wird von der gSMC-K bzw. SM-B durchgeführt. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der gSMC-K bzw. SM-B. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* kann auch im EVG durchgeführt werden. Die entsprechenden öffentlichen Schlüsselobjekte werden entweder im EVG erzeugt (FCS_CKM.1/NK.Zert) oder importiert (FDP_ITC.2/NK.TLS). Die Interpretation von TLS Zertifikaten wird durch FPT_TDC.1/NK.TLS.Zert erbracht.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK für die öffentlichen Schlüsselobjekte zur *verification of digital signatures* im EVG.

FCS_COP.1.1/NK.TLS.Auth The TSF shall perform

a) *verification of digital signatures and*

b) *signature creation with support of gSMC-K or SM-B storing the signing key and performing the RSA operation* [152]

in accordance with a specified cryptographic algorithm *sha256withRSAEncryption OID 1.2.840.113549.1.1.11*[153] and cryptographic key sizes *2048 bit*[154] that meet the following: RFC 8017 *(PKCS#1) [31], FIPS PUB 180-4 [14]*[155].

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

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

[153] [assignment: *cryptographic algorithm*]

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

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

Anwendungshinweis 119: Die Signaturberechnung gemäß FCS_COP.1/NK.TLS.Auth wird für die Berechnung digitaler Signaturen zur Authentisierung bei TLS verwendet. Der EVG nutzt dafür bei Verbindungen ins lokale Netz (LAN) des Leistungserbringers die gSMC-K. Der dafür benötigt asymmetrische Schlüssel kann während der Produktion der gSMC-K importiert oder generiert werden. Es werden deshalb keine spezischen Anforderungen an die Quelle dieses Schlüssels gestellt. Für Verbindungen zum WAN wird eine SM-B verwendet die der Anwendungskonnektor ansteuert. Die WAN-seitige TLS-Verbindung erfolgt analog und nutzt dieselben kryptografischen Basisdienste für TLS.

FCS_CKM.1/NK.Zert Cryptographic key generation / Certificates

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

nicht erfüllt mit folgender Begründung: FCS_CKM.1/NK.Zert bietet die Möglichkeit X.509 Zertifikate für die TLS-geschützte Kommunikation mit Clientsystemen zu Erzeugen. Gemäß FDP_ETC.2/NK.TLS können die Zertifikate und die zugehörigen privaten Schlüssel vom Administrator exportiert werden. Keydistribution gemäß FCS_CKM.2 findet nicht statt.

FCS_CKM.4 Cryptographic key destruction

hier erfüllt durch: FCS_CKM.4/NK

FCS_CKM.1.1/NK.Zert The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment**:** *Algorithm for cryptographic key generation of key pairs*] and specified cryptographic key sizes *2048 bit*[156] that meet the following: *Standard OID 1.2.840.113549.1.1.11, RFC 4055 [35], BSI TR-03116-1 [68]*[157].

The TSF shall

(1) create a valid X.509 [36] certificate with the generated RSA key pair and

(2) create a PKCS#12 [37] file with the created certificate and the associated private key. [158]

Anwendungshinweis 120: Der Algorithmus für die Schlüsselerzeugung muss die Vorgaben aus [74], Anforderung GS-A_4368 umsetzen. Die Verfeinerung zu FCS_CKM.1/NK.Zert soll die Möglichkeit zur Erzeugung von X.509 Zertifikaten für die TLS-geschützte Kommunikation mit Clientsystemen bieten. Ein Export dieser Zertifikate und der zugehörigen privaten Schlüssel ist Gegenstand von FDP_ETC.2/NK.TLS.

FDP_ITC.2/NK.TLS Import of user data with security attributes

156 [assignment: *cryptographic key sizes*]

157 [assignment: *list of standards*]

158 refinement

Import von Zertifikaten

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

Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanaged. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen importiert werden. Die Abhängigkeit wird durch FDP_ACC.1/AK.TLS des Anwendungskonnektors erfüllt.

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

hier erfüllt durch: FTP_TRP.1/NK.Admin

FPT_TDC.1 Inter-TSF basic TSF data consistency

hier erfüllt durch: FPT_TDC.1/NK.TLS.Zert

FDP_ITC.2.1/NK.TLS The TSF shall enforce the *Certificate-Import-SFP*[159] 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 Management-Schnittstelle

(2) [assignment: *additional importation control rules]*. [160]

Anwendungshinweis 121: Gemäß FMT_MOF.1/NK.TLS kann der Netzkonnektor die Steuerung, unter welchen Umständen der Import von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen. Wenn es für den Hersteller aber einfacher ist, dies im Kontext des Netzkonnektors zu beschreiben (etwa weil er eine vom Netzkonnektor gemanagede Schnittstelle dafür verwendet) ist auch dies gemäß FMT_MOF.1/NK.TLS zulässig.

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

Export von Zertifikaten

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

160 [assignment: *additional importation control rules*]

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

Gemäß dem SFR FMT_MOF.1/NK.TLS werden die TLS-Verbindungen des Konnektors durch den Anwendungskonnektor gemanaged. Dies betrifft auch die Bedingungen dafür, wie und wann Schlüssel und Zertifikate für TLS-Verbindungen erzeugt und exportiert werden. Die Abhängigkeit wird durch FDP_ACC.1/AK.TLS des Anwendungskonnektors erfüllt.

FDP_ETC.2.1/NK.TLS The TSF shall enforce the *Certificate-Export-SFP*[161] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/NK.TLS The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/NK.TLS The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/NK.TLS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) *Die TSF exportiert X.509 Zertifikate für Clientsysteme und den zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle. Als Exportformat wird PKCS#12 verwendet.*

(2) *[assignment: additional exportation control rules]*. [162]

Anwendungshinweis 122: Gemäß FMT_MOF.1/NK.TLS kann der Netzkonnektor die Steuerung, unter welchen Umständen der Export von Client-Zertifikaten erfolgt, dem Anwendungskonnektor überlassen. Wenn es für den Hersteller aber einfacher ist, dies im Kontext des Netzkonnektors zu beschreiben (etwa weil er eine vom Netzkonnektor gemanagede Schnittstelle dafür verwendet) ist auch dies gemäß FMT_MOF.1/NK.TLS zulässig.

FMT_MOF.1/NK.TLS Management of security functions behaviour

Management von TLS-Verbindungen durch den Anwendungskonnektor

Dependencies: FMT_SMR.1 Security roles

hier erfüllt durch FMT_SMR.1./NK

FMT_SMF.1 Specification of Management Functions

hier erfüllt durch FMT_SMF.1/NK

FMT_MOF.1.1/NK.TLS The TSF shall restrict the ability to determine the behaviour of[163] the functions *Management of TLS-Connections*

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

162 [assignment: *additional exportation control rules*]

required by the Anwendungskonnektor[164]to *Anwendungskonnektor*[165].

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. **[assignment: *additional rules*]**

If one or more of these rules are managed by the EVG itself, this shall also be interpreted as a fulfillment of this or these rules. [166]

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.

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

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

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

164 [assignment:*list of functions*]

165 [assignment: *the authorised identified roles*]

166 refinement

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

Anwendungshinweis 124: Wenn es für den Hersteller des Netzkonnektors für die Dokumentation zu den Klassen ADV und ATE einfacher erscheint, das im SFR beschriebene Managment der TLS-Verbindungen ganz oder teilweise bereits beim Netzkonnektor anzusiedeln, soll dies ausdrücklich erlaubt sein. In diesem Sinne ist der letzte Satz im SFR zu verstehen. Insbesondere kann er auch einige oder alle auf TLS-Verbindungen bezogenen SFRs aus dem Schutzprofil für den Konnektor hier übernehmen.

6.3. Funktionale Sicherheitsanforderungen des Anwendungskonnektors

6.3.1. Klasse FCS: Kryptographische Unterstützung

Der EVG implementiert kryptographische Algorithmen in der Software des Konnektors. Die asymmetrischen Algorithmen mit privaten Schlüsseln und die kryptographischen Algorithmen und Protokolle für die Kommunikation mit Chipkarten (d. h. dem HBA für Stapelsignatur) 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.

Für alle Kryptoalgorithmen gelten die Festlegungen der TR-03116 [68] und der gematik-Spezifikation zu den anzuwendenden Kryptoalgorithmen [74].

Anwendungshinweis 125: Es gilt Anwendungshinweis 109.

6.3.1.1. Basisalgorithmen

Der Konnektor nutzt kryptographische Dienste der gSMC-K, in der Einsatzumgebung. Das PP COS [70] fordert die Evaluierung der kryptographischen Funktionen des Betriebssystems der gSMC-K, die durch das Objektsystem der gSMC-K ausgewählt werden.

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[167] in accordance with a specified cryptographic algorithm SHA-256, SHA-512/256, SHA-384 und SHA-512[168] and cryptographic key sizes none[169] that meet the following: Standard FIPS PUB 180-4 [14][170].

Anwendungshinweis 126: Die Hashfunktion SHA-256 wird 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.

FCS_CKM.1/AK.AES Cryptographic key generation / AES keys

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ AK.AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment**:** *Algorithm for cryptographic key generation **of AES keys***] and specified cryptographic key sizes 128 bit and 256 bit[171] that meet the following: [assignment: *list of standards*].

Anwendungshinweis 128: Die Sicherheitsvorgaben müssen die Zuweisung zum Schlüssel-Erzeugungsalgorithmus ausführen. Der EVG muss Schlüssel mit einer Entropie von mindestens 100 Bit erzeugen (siehe [68]). Nach [15] sind keine schwachen Schlüssel für den AES bekannt. Der EVG soll alle Schlüsselbits durch den Zufallszahlengenerator gemäß der Einsatzumgebung erzeugen, um eine maximale Entropie zu erreichen und keine Schwachstelle gegenüber der möglichen kryptographischen Stärke des AES zu bilden.

167 [assignment: *list of cryptographic operations*]

168 [assignment: *cryptographic algorithm*]

169 [assignment: *cryptographic key sizes*]

170 [assignment: *list of standards*]

171 [assignment: *cryptographic key sizes*]

FCS_CKM.4/AK	**Cryptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CMK.4.1/AK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meet the following: [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] [42], CAdES [26] [43], PAdES [27] [44] 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[172] in accordance with a specified cryptographic algorithm RSASSA-PKCS1-v1_5 signature verification[173] and cryptographic key sizes 1976 bit to 4096 bit[174] that meet the following: Standard PKCS#1 [31][175].

Anwendungshinweis 129: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.SSA wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet [74], Kap. 6.1.

172 [assignment: *list of cryptographic operations*]

173 [assignment: *cryptographic algorithm*]

174 [assignment: *cryptographic key sizes*]

175 [assignment: *list of standards*]

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.

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[176] in accordance with a specified cryptographic algorithm RSASSA-PSS signature verification[177] and cryptographic key sizes 1976 bit to 4096 bit[178] that meet the following: Standard PKCS#1v2.2, [31][179].

Anwendungshinweis 131: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.PSS wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet [74], Kap. 6.1.

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.

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[180] in accordance with a specified cryptographic algorithm ECDSA[181] and cryptographic key sizes 256 bit[182] that meet the following: Standard TR-03111 [66][183].

176 [assignment: *list of cryptographic operations*]

177 [assignment: *cryptographic algorithm*]

178 [assignment: *cryptographic key sizes*]

179 [assignment: *list of standards*]

180 [assignment: *list of cryptographic operations*]

181 [assignment: *cryptographic algorithm*]

Anwendungshinweis 133: Die Signaturprüfung gemäß FCS_COP.1/AK.SigVer.ECDSA wird für die Prüfung qualifizierter elektronischer Signaturen und nicht-qualifizierten elektronischen Signaturen verwendet [74], Kap. 6.1.

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[184] **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm (1) XML Advanced Electronic Signature (XAdES), (2) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS[185] and cryptographic key sizes no key[186] that meet the following: Standards XMLSig [22], XAdES[25] [42] and FIPS PUB 180-4 [14][187].

Anwendungshinweis 134: FCS_COP.1/AK.XML.Sign fordert die Erzeugung von XML-Signaturen nach vorgegebenen Signaturrichtlinein 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 (sowie zukünftig ECDSA), geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel.

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]

182 [assignment: *cryptographic key sizes*]

183 [assignment: *list of standards*]

184 [assignment: *list of cryptographic operations*]

185 [assignment: *cryptographic algorithm*]

186 [assignment: *cryptographic key sizes*]

187 [assignment: *list of standards*]

	FCS_CKM.4 Cryptographic key destruction
FCS_COP.1/ AK.CMS.Sign	The TSF shall perform sign documents[188] **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 [189] and cryptographic key sizes no key[190] that meet the following: Standards RFC5652[33], CAdES [26] [43] and FIPS PUB 180-4 [14][191].

Anwendungshinweis 135: FCS_COP.1/AK.CMS.Sign fordert die Erzeugung von CMS-Signaturen nach vorgegebenen Signaturrichtlinein. Die Verfeinerung hebt hervor, dass bestimmte Anteile durch den EVG (insbesondere die Hashfunktion gemäß FCS_COP.1/AK.SHA) und andere Teile durch die Signaturchipkarten der Einsatzumgebung, insbesondere die Erzeugung der digitalen Signatur gemäß RSA mit PKCS#1v2.2 RSASSA-PSS und RSA 2048 Bit-Schlüsseln (sowie zukünftig ECDSA), geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel. Die CMS-Signaturen werden ebenfalls in S/MIME-Nachrichten verwendet.

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/ AK.PDF.Sign	The TSF shall perform sign PDF-A documents[192] **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[193] and cryptographic key sizes no key[194] that meet the following: Standards PAdES [27] [44] and FIPS PUB 180-4 [14][195] .

188 [assignment: *list of cryptographic operations*]

189 [assignment: *cryptographic algorithm*]

190 [assignment: *cryptographic key sizes*]

191 [assignment: *list of standards*]

192 [assignment: *list of cryptographic operations*]

193 [assignment: *cryptographic algorithm*]

194 [assignment: *cryptographic key sizes*]

195 [assignment: *list of standards*]

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 (sowie zukünftig ECDSA), geleistet werden. Der EVG selbst benötigt für diese kryptographische Operation keine Schlüssel.

FCS_COP.1/AK.XML.SigPr	**Cryptographic operation / XML signature verification**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ AK.XML.SigPr	The TSF shall perform verify signed XML documents[196] in accordance with a specified cryptographic algorithm (1) XML Advanced Electronic Signature (XAdES), (2) SHA-256, SHA-512/256, SHA-384 and SHA-512 according to FCS_COP.1/AK.SHA with RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA, RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS[197] and cryptographic key sizes 1976 bit to 4096 bit for RSA[198], (3) SHA-256 und SHA-512/256 mit ECDSA according to FCS_COP.1/AK.SigVer.ECDSA[199] and cryptographic key sizes 256 bit**[200]** that meet the following: Standards XMLSig[21], XAdES [25] [42], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [66][201].

Anwendungshinweis 137: FCS_COP.1/AK.XML.SigPr fordert die Prüfung von XML-Signaturen nach vorgegebenen Signaturrichtlinien und den bereits oben spezifizierten Kryptoalgorithmen. Die Prüfung mit anderen Signaturalgorithmen soll unterstützt werden, insbesondere mit solchen, die bei der Erstellung neuer elektronischer Signaturen unzulässig wären. In diesen Fällen soll der Nutzer in geeigneter Weise informiert werden.

196 [assignment: *list of cryptographic operations*]

197 [assignment: *cryptographic algorithm*]

198 [assignment: *cryptographic key sizes*]

199 [assignment: *cryptographic algorithm*]

200 [assignment: *cryptographic key sizes*]

201 [assignment: *list of standards*]

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[202] in accordance with a specified cryptographic algorithm (1) CMS Advanced Electronic Signature (CAdES), (2) SHA-256, SHA-512/256, SHA-384 and SHA-512 according to FCS_COP.1/AK.SHA with RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA, RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS[203] and cryptographic key sizes 1976 bit to 4096 bit for RSA[204], (3) SHA-256 and SHA-512/256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA[205] and cryptographic key sizes 256 bit[206] and cryptographic key sizes only 2048 bit for RSA[207] that meet the following: Standards RFC5652[33], CAdES [26] [43], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [66][208].

Anwendungshinweis 138: FCS_COP.1/AK.CMS.SigPr fordert die Prüfung von CMS-Signaturen nach vorgegebenen Signaturrichtlinein und den bereits oben spezifizierten Kryptoalgorithmen. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_COP.1/AK.PDF.SigPr	**Cryptographic operation / PDF signature verification**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes,

202 [assignment: *list of cryptographic operations*]

203 [assignment: *cryptographic algorithm*]

204 [assignment: *cryptographic key sizes*]

205 [assignment: *cryptographic algorithm*]

206 [assignment: *cryptographic key sizes*]

207 [assignment: *cryptographic key sizes*]

208 [assignment: *list of standards*]

	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[209] in accordance with a specified cryptographic algorithm (1) PAdES [27] [44], (2) SHA-256, SHA-512/256, SHA-384 and SHA-512 according to FCS_COP.1/AK.SHA with RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA, RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS[210] and cryptographic key sizes 1976 bits to 4096 bits for RSA[211], (3) SHA-256 and SHA-512/256 with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA[212] and cryptographic key sizes 256 bit[213] and cryptographic key sizes only 2048 bit for RSA[214] that meet the following: Standards PAdES [27] [44], FIPS PUB 180-4, PKCS#1 [31] and TR-03111 [66][215].

Anwendungshinweis 139: FCS_COP.1/AK.PDF.SigPr fordert die Prüfung von PDF-Signaturen nach vorgegebenen Signaturrichtlinein und den bereits oben spezifizierten Kryptoalgorithmen. Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

FCS_COP.1/AK.PKCS.SigPr	**Cryptographic operation / PKCS 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.PKCS.SigPr	The TSF shall perform verify signed binary data[216] in accordance with a specified cryptographic algorithm

209 [assignment: *list of cryptographic operations*]

210 [assignment: *cryptographic algorithm*]

211 [assignment: *cryptographic key sizes*]

212 [assignment: *cryptographic algorithm*]

213 [assignment: *cryptographic key sizes*]

214 [assignment: *cryptographic key sizes*]

215 [assignment: *list of standards*]

(1) PKCS#1v2.2 RSASSA-PKCS1-v1_5,

(2) PKCS#1v2.2 RSASSA-PSS,

(3) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS[217]

and cryptographic key sizes [assignment: *cryptographic key sizes*][218] that meet the following: RFC 8017 [31] and FIPS PUB 180-4 [14][219].

Anwendungshinweis 140: Für die Prüfung von Signaturen ist die Verwendung veralteter Algorithmen und Parameter erlaubt, sofern die Algorithmen bzw. Parameter zum Signaturerstellungszeitpunkt noch gültig waren.

216 [assignment: *list of cryptographic operations*]

217 [assignment: *cryptographic algorithm*]

218 [assignment: *cryptographic key sizes*]

219 [assignment: *list of standards*]

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 [220] in accordance with a specified cryptographic algorithm AES-GCM[221] and cryptographic key sizes 128 bit, 192 bit and 256 bit[222] that meet the following: Standards FIPS 197 [15], NIST-SP-800-38A [16][223].

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 128 Bit und 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.

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[224] in accordance with a specified cryptographic algorithm RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit[225] and cryptographic key sizes 256 bit for AES and 2048 bit for RSA[226] that meet the following: Standards NIST-SP-800-38D [17], PKCS#1 [31],

220 [assignment: *list of cryptographic operations*]

221 [assignment: *cryptographic algorithm*]

222 [assignment: *cryptographic key sizes*]

223 [assignment: *list of standards*]

224 [assignment: *list of cryptographic operations*]

225 [assignment: *cryptographic algorithm*]

226 [assignment: *cryptographic key sizes*]

FIPS 197 [15] und XMLEnc [21][227].

Anwendungshinweis 142:

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[228] in accordance with a specified cryptographic algorithm [**Selection:** RSA RSAES-PKCS1-v1_5, RSAOAEP] and AES-GCM with authentication tag length of 128 bit[229] and cryptographic key sizes 128 bit, 192 bit and 256 bit[230] that meet the following: Standards NIST-SP-800-38D [17], FIPS 197 [15] und XMLEnc [21][231].

Anwendungshinweis 143: Die asymmetrische Entschlüsselung des AES-Schlüssels mit privaten Schlüsseln gemäß [74] und [70] erfolgt durch die Chipkarte der Einsatzumgebung (HBA, SMC-B oder ggf. eGK).

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[232] in accordance with a specified cryptographic algorithm RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit[233] and cryptographic

227 [assignment: *list of standards*]

228 [assignment: *list of cryptographic operations*]

229 [assignment: *cryptographic algorithm*]

230 [assignment: *cryptographic key sizes*]

231 [assignment: *list of standards*]

232 [assignment: *list of cryptographic operations*]

233 [assignment: *cryptographic algorithm*]

	key sizes 256 bit for AES and 2048 bit for RSA[234] that meet the following: Standards NIST-SP-800-38D [17], PKCS#1 [31], FIPS 197 [15] und RFC 5751 [34][235].

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[236] in accordance with a specified cryptographic algorithm [**Selection:** RSA RSAES-PKCS1-v1_5, RSAOAEP] and AES-GCM with authentication tag length of 128 bit[237] and cryptographic key sizes 128 bit, 192 bit and 256 bit[238] that meet the following: Standards NIST-SP-800-38D [17], PKCS#1 [31], FIPS 197 [15] und RFC 5751 [34][239].

Anwendungshinweis 144: Die asymmetrische Entschlüsselung des AES-Schlüssels gemäß [74] und [70] 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 [63] mit AES-GCM Inhaltsverschlüsselung gemäß RFC 5084 [64] verwendet werden.

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[240] in accordance with a specified cryptographic

234 [assignment: *cryptographic key sizes*]

235 [assignment: *list of standards*]

236 [assignment: *list of cryptographic operations*]

237 [assignment: *cryptographic algorithm*]

238 [assignment: *cryptographic key sizes*]

239 [assignment: *list of standards*]

240 [assignment: *list of cryptographic operations*]

	algorithm RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit[241] and cryptographic key sizes 256 bit for AES and 2048 bit for RSA[242] that meet the following: Standards NIST SP800-38D [17], PKCS#1 [31], FIPS 197 [15] and CMS [33][243].

Anwendungshinweis 146:

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[244] in accordance with a specified cryptographic algorithm [**Selection:** RSA RSAES-PKCS1-v1_5, RSAOAEP] and AES-GCM with authentication tag length of 128 bit[245] and cryptographic key sizes 128 bit, 192 bit and 256 bit[246] that meet the following: Standards NIST SP800-38D [17], PKCS#1 [31], FIPS 197 [15] and CMS [33][247].

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 [assignment: a defined quality metric].

241 [assignment: *cryptographic algorithm*]

242 [assignment: *cryptographic key sizes*]

243 [assignment: *list of standards*]

244 [assignment: *list of cryptographic operations*]

245 [assignment: *cryptographic algorithm*]

246 [assignment: *cryptographic key sizes*]

247 [assignment: *list of standards*]

Anwendungshinweis 147: Die Verfeinerung von „Geheimnisse“ zu „Passwörtern“ ist notwendig, um die Qualitätsanforderungen gegenüber anderen Mechanismen abzugrenzen. Gemäß [76], Kap. 4.3.1, sind Administratorpasswörter gefordert, die den Anforderungen aus dem IT_Grundschutz-Katalog des BSI genügen. Mindestens diese Anforderungen sind vom ST-Autor durch das assignment "a defined quality metric" in FIA_SOS.1/AK**.Passwörter** umzusetzen.

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[248].
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[249].

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) [assignment: *list of TSF-mediated actions*][250] 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: Der Autor der Sicherheitsvorgaben kann weitere TSF-vermittelte Aktionen zuweisen, sofern diese nicht durch dieses Schutzprofil beschrieben sind und diesem nicht widersprechen. Der EVG identifiziert den Benutzer EVG implizit über die benutzte Schnittstelle.

FIA_UAU.1/AK	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1/AK	The TSF shall allow

248 [assignment: *a defined quality metric*]

249 [assignment: *list of TSF functions*]

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

(1) Identification of an user of the administrative interface, an user of the a Clientsytem, a smart card and an 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) [assignment: *list of TSF mediated actions*][251]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/AK The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Anwendungshinweis 149: Der Autor der Sicherheitsvorgaben kann weitere TSF-vermittelte Aktionen zuweisen, sofern diese nicht durch dieses Schutzprofil beschrieben sind und diesem nicht widersprechen. 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) [selection: *password based authentication mechanism*, *[assignment: another authentication mechanism]*] for administrator users,

(2) TLS authentication with a pairing secret for eHKT [76], 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[252].

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

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

[252] [assignment: *list of multiple authentication mechanisms*]

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[253].

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.

253 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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[254] to prove the identity of the "SAK"[255].

Anwendungshinweis 151: Diese SFR ergibt sich aus der TR-03114 [67] und den Zugriffsbedingungen des HBA, die für eine Stapelsignatur die Authentisierung der Identität „SAK" gegenüber dem HBA und die Übermittlung der DTBS mit Secure Messaging erfordern. Die gSMC-K muss dafür über ein CVC mit der CHAT für die Identität „SAK" (vergl. C.SAK.AUTD_CVC in [84]) 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 [67], [80], [82] und [84] 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 Tabellen im Abschnitt 7.1 des vorliegenden Schutzprofils.

FDP_ACC.1/AK.Infomod	**Subset access control / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK.Infomod	The TSF shall enforce the Infomodell-SFP[256] on the subject S_Clientsystem, the objects as in TAB_KON_507, and the operation:

254 [assignment: *authentication mechanism*]

255 [assignment: *identity or role*]

- usage of the resource (the object) in a technical use case

[257].

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[258] to objects based on the following: the subject S_Clientsystem with its associated security attributes defined in Tabelle 12, and the objects with their associated security attributes defined in TAB_KON_508 and TAB_KON_509[259].
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.[260]
FDP_ACF.1.3/AK**.**Infomod	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[261].
FDP_ACF.1.4/AK**.**Infomod	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[262].

FMT_MSA.1/AK.Infomod	**Management of security attributes / Informationsmodell**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.

256 [assignment: *access control SFP*]

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

258 [assignment: *access control SFP*]

259 [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*]

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

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

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

FMT_MSA.1.1/AK.Infomod	The TSF shall enforce the Infomodell-SFP[263] to restrict the ability to modify, delete, create[264] 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[265] to S_Administrator[266].

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[267] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] [268] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AK.Infomod	The TSF shall allow the [Selection: S_Administrator, *no role*][269] 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

263 [assignment: *access control SFP(s), information flow control SFP(s)*]

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

265 [assignment: *list of security attributes*]

266 [assignment: *the authorised identified roles*]

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

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

269 [assignment: *the authorised identified roles*]

FDP_ACC.1.1/AK.eHKT The TSF shall enforce the Kartenterminaldienst-SFP[270] 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;
[271].

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 [76] und [77] beschrieben. Die gesamte Kommunikation des Konnektors mit den eHealth-Kartenterminals erfolgt über die TLS-Kanäle des Kartenterminaldienstes.

270 [assignment: *access control SFP*]

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

Operation	Beschreibung	Anmerkung
TLS-Kanal abbauen	Freigabe der Resourcen des TLS-Kanals gemäß FDP_RIP.1/AK und Löschen der symmetrischen Schlüssel gemäß FCS_CKM.4/AK	Die eHealth-Kartenterminals setzen die gesteckten Chipkarten bei Abbau des TLS-Kanals zurück.
Senden eines SICCT-Kommando anfordern	Übergabe eines SICCT-Kommandos zur Übermittlung an eHealth-Kartenterminals	
SICCT-Kommando senden	Übermittlung eines SICCT-Kommandos gemäß [79] und [77]über den TLS-Kanal an ein eHealth-Kartenterminal,das durch den Chipkartendienst selbst erzeugt oder an den Kartenterminaldienst übergeben wurde	Die SICCT-Kommandos dienen [77] [79] - der Steuerung des eHealth-Kartenterminals, insbesondere zur Kommunikation mit dem Konnektor, Kommandoabarbeitung und Konfiguration der eHealth-Kartenterminals, - dem Zugriff auf die sichere Anzeige (Display und Anzeige des gesicherten PIN-Modus), und die Tastatur sowie ggf. dem Tongeber, - der Kontrolle, Aktivierung, Deaktivierung und Statusabfrage des elektrischen Zustands von Chipkartenkontaktiereinheiten und der Kommunikation mit Chipkarten in den Chipkartenslots, und - die Auslösung der Prozesse zur PIN-Eingabe und dem PIN-Wechsel im gesicherten Modus.
Antwort auf SICCT-Kommando empfangen	Empfangen der Antworten auf ein selbst gebildetes oder übergebenes SICCT-Kommando	

Tabelle 15: 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 [272] 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 [273].
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-

[272] [assignment: *access control SFP*]

[273] [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*]

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.

.[274]

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.[275]

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) [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*][276]

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

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

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

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

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[277] to transmit and receive[278] ~~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[279] to transmit and receive[280] user data ~~**in a manner**~~ protected from modification, deletion, insertion, replay[281] errors.
FDP_UIT.1.2/AK**.**TLS	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, replay[282] 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[283] the Arbeitsplatzkonfigurationsdaten: (1) Name eines zugelassenen eHealth-Kartenterminals, (2) Statische IP-Adresse eines zugelassenen eHealth-Kartenterminals,

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

278 [selection: *transmit, receive*]

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

280 [selection: *transmit, receive*]

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

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

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

(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
.[284]

to S_AK and S_Administrator[285].

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[286] 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 .[287] to S_Administrator[288].

284 [assignment: *list of TSF data*]

285 [assignment: *the authorised identified roles*]

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

287 [assignment: *list of TSF data*]

288 [assignment: *the authorised identified roles*]

Anwendungshinweis 152: Die Iteration differenziert die Zugriffsbedingungen für das Management der Konfigurationsdaten nach Zugriffsarten und Rollen. Das Management der Kartenterminals ist in [76] 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 [76], 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. [76]). 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[289] 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,

289 [assignment: *access control SFP*]

(9) auf Kartenobjekte zugreifen,
(10) Chipkartenkommando übertragen und Antwort empfangen,
(11) Benutzerauthentisierung anfordern
.[290]

Operation	Beschreibung	Anmerkung
Kartenhandle ausgeben	Für eine neu gesteckte Chipkarte wird ein eindeutiges Kartenhandle gebildet und an den EVG ausgegeben.	Die mit dem Kartenhandle verknüpften Informationen können folgende Sicherheits-attribute der Chipkarte enthalten: Identität des Kartenslots, Identität des eHealth-Kartenterminals, Identität des Arbeitsplatzes, dem das eHealth-Kartenterminal zugeordnet ist.
Logischen Kanal anfordern	Für eine mit dem Kartenhandle identifizierte Chipkarte wird ein logischer Kanal angefordert.	Der EVG kann mit einem Kartenhandle einen neuen logischen Kanal anfordern.
Logischen Kanal öffnen	Für eine mit dem Kartenhandle identifizierte Chipkarte wird ein logischer Kanal 1, 2 oder 3 geöffnet (Chipkartenkommando MANAGE CHANNEL).	Der EVG kann mit einem Kartenhandle einen neuen logischen Kanal anfordern.
Logichen Kanal schließen	Wenn der identifizierte logische Kanal der Kanal 0 ist, so ist der Sicherheitszustand dieses logischen Kanals zurückzusetzen. Wenn der identifizierte logische Kanal ein Kanal 1, 2 oder 3 ist, so ist der logische Kanal zu schließen (Chip kartenkommando MANAGE CHANNEL).	
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.	

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

Digitale Signatur erstellen	Erstellen digitaler Signturen mit privaten Signaturschlüsseln und den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT und PSO COMPUTE DIGITAL SIGNATURE.	Die Zugriffsregeln der Chipkarten entscheiden, ob das Kommando PSO COMPUTE DIGITAL SIGNATURE für den kryptographischen Schlüssel zulässig ist.
Chiffrate entschlüsseln	Entschlüsseln von Chiffraten mit privaten Entschlüsselungsschlüsseln und den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT und PSO DECIPHER.	Die Zugriffsregeln der Chipkarten entscheiden, ob das Kommando PSO DECIPHER für den kryptographischen Schlüssel zulässig ist.
Auf Kartenobjekte zugreifen	Zugriff auf Datenobjekte der Chipkarten. Es wird zwischen lesendem und schreibenden Zugriff auf eine Datei bzw. Record, der Suche und dem Hinzufügen von Records unterschieden.	Die Chipkarten außer KVK verfügen über eine eigene Zugriffskontrolle auf Kartenobjekte.
Chipkarten-kommando übertragen und Antwort empfangen	Übertragung von Chipkarten-kommandos und das Empfangen von Antworten innerhalb von SICCT-Kommandos des Kartenterminal-dienstes	
Benutzerauthentisierung anfordern	Anforderung von Benutzerinteraktionen zur PIN-Authentisierung, PIN-Änderung, PIN-Entsperren, der Freischaltung einer SM-B durch einen HBA und die Abfrage des PIN-Status auslösen und die Rückantwort der Chipkarten zurückerhalten.	

Tabelle 16: 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[291] 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”

.[292]

FDP_ACF.1.2/AK.KD

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Der S_Chipkartendienst erzeugt für jede neu gesteckte Chipkarte ein Kartenhandle und übergibt für identifizierte eGK, SMC-B und HBA den im gespeicherten X.509 angegeben Namen des Kartenhalters an das Subjekt S_AK.

(2) Die Subjekte S_AK und S_Fachmodul dürfen einen neu zu öffnenden 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

291 [assignment: *access control SFP*]

292 [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*]

mit dem Kartenhandle identifizierten Chipkarte anfordern. Wenn die identifizierte Chipkarte einen logischen Kanal bereitstellt, öffnet der Chipkartendienst einen solchen logischen Kanal.

(4) Nur die Subjekte S_AK, S_Signaturdienst und S_Fachmodul dürfen die Card-to-Card-Authentisierung zwischen zwei logischen Kanäle verschiedener Chipkarten anfordern. Nur das Subjekt Chipkartendienst darf die Card-to-Card-Authentisierung für logische Kanäle durchführen.

(5) Nur der Signaturdienst darf mit den Chipkarten digitale Signaturen für QES und non-QES mit den Kommandos MANAGE SECURITY ENVIRONMENT und PSO COMPUTE DIGITAL SIGNATURE erzeugen.

(6) Nur der Verschlüsselungsdienst darf mit den Chipkarten Kommandos MANAGE SECURITY ENVIRONMENT und PSO DECIPHER auf Chipkarten zugreifen.

(7) Das Subjekt S_AK darf mit den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT, INTERNAL AUTHENTICATE, PSO COMPUTE DIGITAL SIGNATURE und GENERATE ASYMMETRIC KEY PAIR P1='81' auf den Schlüssel PrK.HCI.AUT zugreifen, wenn der Zugriff zu einem logischen Kanal einer SM-B gehört

(8) Nur der Chipkartendienst, der Signaturdienst, und der Verschlüsselungsdienst dürfen über einen logischen Kanal zu einer Chipkarte die Chipkartenkommandos MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE und MUTUAL AUTHENTICATE absetzen.

(9) Die Subjekte S_AK und S_Fachmodul, dürfen die Schließung des vom jeweiligen Subjekt angeforderten logischen Kanals anfordern. Der Chipkartendienst setzt den Sicherheitsstatus des logischen Kanals zurück.

(10) Der Chipkartendienst löscht das Kartenhandle, wenn die betreffende Chipkarte gezogen wird.

(11) Fachmodule und Clientsysteme können sich für die Ereignisse „CARD INSERTED", „CARD REMOVED", „CARD PIN VERIFY_STARTED", „CARD PIN VERIFY_FINISHED", „CARD PIN CHANGE_STARTED", „CARD PIN

CHANGE_FINISHED“, "CARD PIN ENABLE_STARTED", "CARD PIN ENABLE_FINISHED", "CARD PIN DISABLE_STARTED" und "CARD PIN DISABLE_FINISHED" registrieren, um bei Eintritt der Ereignisse informiert zu werden.

(12) Das Clientssystem darf eine Benutzerauthentisierung anfordern.[293]

FDP_ACF.1.3/AK.KD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[294]

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

.[295]

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 [76], Kap. 4.1.5.4, definiert.

FDP_ACC.1/AK.PIN	**Subset access control / PIN**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK.PIN	The TSF shall enforce the VAD-SFP[296] on

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

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

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

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
.[297]

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	Die an den äußeren Schnittstellen sichtbaren Prozesse der lokalen

296 [assignment: *access control SFP*]

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

	Chipkarte, der zu verwendende PIN-Referenz und der Funktion gemäß der Anforderung.	PIN-Eingabe sind in [76], 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 [76], Kap. 4.1.5, und [67] 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 [79] und [77] beschrieben.

Tabelle 17: 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[298] 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 .[299]

298 [assignment: *access control SFP*]

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

299 [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*]

gSMC-KT übergibt und nur die verschlüsselte VAD innerhalb des TLS-Kanals an den Konnektor übermittelt,

(iii) das Chipkartenterminal die verschlüsselte VAD nur für die PIN-Prüfung, das PIN-Entsperren oder den PIN-Wechsel dem als PIN-Empfänger authentisierten Heilberufsausweis oder der als PIN-Empfänger authentisierten SMC-B übergibt;

(b) wenn das PIN-Terminal und das Chipkarten-Terminal identisch sind, das PIN-Terminal die eingegebene VAD im Klartext nur für die PIN-Prüfung, PIN-Aktivierung, PIN-Deaktivierung, das PIN-Entsperren oder den PIN-Wechsel an die authentisierte eGK, den Heilberufsausweis und die SMC-B übergibt,

(c) die PIN-Eingabe am PIN-Terminal nur im gesicherten Mode erfolgt.[300]

FDP_ACF.1.3/AK**.**PIN The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

FDP_ACF.1.4/AK**.**PIN The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Kein Subjekt außer dem Chipkartendienst darf über den TLS-Kanal des EVG zu den eHealth-Kartenterminals SICCT-Kommandos mit dem Chipkartenkommando VERIFY, RESET RETRY COUNTER, DISABLE VERIFICATION 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) [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*][301]

Die durch **FDP_ACC.1/AK.PIN** und FDP_ACF.1/AK**.PIN** verwendeten Operationen sind in Tabelle 17 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. [76]) durch das Clientsystem ist nicht gestattet.

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

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

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 [302].
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 [303].

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. [76], Kap. 4.1.8.1.3). Dies entspricht $1{,}76 \cdot 10^7$ möglichen Jobnummern. Laut [76] wird die Jobnummer vom Konnektor erzeugt und kann durch Clientsysteme abgerufen werden. Der Konnektor soll jedoch laut [76] 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[304] on subjects: (1) S_AK, (2) S_Signaturdienst, (3) S_Benutzer_Clientsystem; objects: (1) Zu signierende Dokumente,

302 [assignment: *a defined quality metric*]

303 [assignment: *list of TSF functions*]

304 [assignment: *access control SFP*]

(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
.[305]

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 Signatur-schlüssel erzeugt wurde. Bei Übereinstimmung sind die Dokumente gültig signiert, sonst sind sie ungültig signiert.
Signierte Dokumente erstellen	Erzeugen einer oder mehrer signierter Dokumente gemäß FDP_DAU.2/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

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

		festgestellten ungültig signierten Dokumente wird der Signatur-PIN-Authentisierungsstatus der Signaturkarte zurücksetzen.

Tabelle 18: 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[306] 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. .[307]
FDP_ACF.1.2/AK.Sgen	The TSF shall enforce the following rules to determine if an

306 [assignment: *access control SFP*]

307 [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*]

operation among controlled subjects and controlled objects is allowed:

(1) Das Subjekt S_AK darf nur nicht autorisierte zu signierende Dokumente an das Subjekt Signaturdienst übergeben und die zu verwendende Signaturrichtlinie, den Signierenden, den Arbeitsplatz und die Signaturkarte identifizieren.

(2) Nur das Subjekt S_Signaturdienst steuert den Signaturprozess des identifizierten Arbeitsplatzes.

(3) Das Subjekt S_Signaturdienst darf nur dann die zu signierenden Dokumente signieren, wenn

  (a) der Sicherheitsstatus der Signaturchipkarte die Erzeugung der digitalen Signatur erlaubt.

(4) Wenn die identifizierte Signaturrichtlinie die Erzeugung einer qualifizierte elektronische Signatur fordert, dann

  (a) muss das Subjekt S_AK den Signierenden und den Arbeitsplatz identifizieren,

  (b) muss die identifizierte Signaturrichtlinie für eine qualifizierte elektronische Signatur geeignet sein,

  (c) muss das Subjekt S_Signaturdienst für die Einfachsignatur die lokale Eingabe der QES-PIN an HBAx oder die entfernte Eingabe der QES-PIN an HBA steuern und für die Stapelsignatur die lokale oder entfernte PIN-Eingabe für HBA steuern,

  (d) darf das Subjekt S_Signaturdienst nur für durch den HBA „autorisierten Benutzer des Clientsystems“ zu signierenden Dokumente Signaturen mit der Signaturkarte erstellen, Signaturen ungültig signierter Dokumente sind zu löschen,

  (e) das Subjekt S_Benutzer_Clientsystem darf den Signaturvorgang für die autorisierten zu signierenden Dokumente abbrechen,

  (f) der S_Signaturdienst darf nur ordnungsgemäß signierte Dokumente an den S_AK zurückgeben,

  (g) das Subjekt S_Signaturdienst muss nach Abarbeitung des Stapels, bei Abbbruch des Signaturvorgangs durch das Subjekt S_Benutzer_Clientsystem und bei festgestellten ungültig signierten Dokumente den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA zurücksetzen.

(5) Wenn die gültige Signaturrichtlinie die Erstellung einer qualifizierten elektronischen Signatur verlangt, darf das Subjekt S_Signaturdienst nur ordnungsgemäße qualifizierte elektronische Signaturen

an den S_AK zurück geben.

(6) Das Subjekt S_AK darf dem S_Signaturdienst Binärstrings mit der maximalen Länge von 512 Bit nur für Signaturen gemäß dss:SignatureType=PKCS#1-Signatur und 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. [308]

FDP_ACF.1.3/AK.Sgen The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/AK.Sgen The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn der S_AK für die zu signierenden Dokumente eine Signaturrichtlinie zur Erstellung qualifizierter elektronische Signatur identifiziert, aber

(a) der Signierende keine qualifizierte elektronische Signatur erzeugen kann oder

(b) die Autorisierung des S_Benutzer_Clientsystem fehlschlägt.

(2) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn für diese zu signierenden Dokumente und den Signierenden die identifizierte Signaturrichtlinie ungültig ist.

(3) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für den Signaturstapel verweigern und alle für zu signierende Dokumente des Signaturstapels bereits erzeugten Signaturen löschen, wenn die Überprüfung der Signatur wenigstens einer signierten Datei des Signaturstapels fehlschlägt.

(4) Außer dem S_Signaturdienst darf kein Subjekt auf

(a) das Verzeichnis DF.QES des HBA,

(b) den Schlüssel PrK.HCI.OSIG der SMC-B,

(c) [assignment: *weitere Signaturschlüssel externer Signaturchipkarten*]

zugreifen.

(5) [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to*

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

objects].

.[309]

Anwendungshinweis 156: Die Spezifikation Konnektor beschreibt die Schnittstelle zwischen dem Clientsystem und dem Konnektor zur Signaturerstellung und die Kartenhandle zur Identifikation einer gesteckten Chipklarte in Verbindung mit einem Arbeitsplatz des Benutzers. Der EVG kann die Signaturkarte des Signierenden mittels Kartenhandle identifizieren. Der EVG kann den Signierenden und den zu benutzenden Arbeitsplatz identifizieren.

Anwendungshinweis 157: Die Bedingungen für die Sicherheitsattribute signierter Dateien „ordungsgemäß“ und „ungültig“ sind durch FMT_MSA.4/AK festgelegt.

Anwendungshinweis 158: Die SFR FDP_ACF.1/AK.Sgen bezieht sich auf die in diesem PP beschriebenen Signaturarten. Sollen vom EVG weitere Signaturarten – bspw. Komfortsignatur – umgesetzt werden, kann in Abstimmung mit der Zertifizierungsstelle für diese Signaturarten teilweise von der SFR abgewichen werden – bspw. FDP_ACF.1.2/AK.Sgen Regel (4)(g).

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[310] on
subjects:
(1) S_AK,
(2) S_Signaturdienst,
(3) S_Benutzer_Clientsystem;
objects:
(1) Signierte Dokumente,
(2) Signaturprüfungsergebnis;
operations:
(1) Signatur prüfen,
(2) Festlegen des angegebenen Zeitpunkts
[311] .

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	Dies ist für die Prüfung qualifizierte elektronische Signaturen gefordert.

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

310 [assignment: *access control SFP*]

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

	den signierten Dokumente fehlt oder von diesem abweichen soll.	

Tabelle 19: 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[312] 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 .[313]
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. [314].
FDP_ACF.1.3/AK.SigPr	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
FDP_ACF.1.4/AK.SigPr	The TSF shall explicitly deny access of subjects to objects based on

312 [assignment: *access control SFP*]

313 [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*]

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

the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

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 anzunehmende Signaturzeitpunkts erfolgt entsprechend [76] hierarchisch:

- Für die QES-Signaturprüfung:
  - falls vorhanden Benutzerdefinierter_Zeitpunkt, sonst
  - falls vorhanden Ermittelter_Signaturzeitpunkt_Eingebettet, sonst
  - optional: falls vorhanden Ermittelter_Signaturzeitpunkt_Qualifiziert, 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 ist die Auswertung von qualifizierten Zeitstempeln (Ermittelter_Signaturzeitpunkt_Qualifiziert) optional. Ein gegebenenfalls vorhandener qualifizierter Zeitstempel kann also entweder ausgewertet werden – und muss dann vollständig geprüft werden – oder er wird 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[315] **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 [41] oder ISO-8859-15 [11]),** **(2) TIFF-Dateien [40],** **(3) Adobe Portable Document Format (PDF/A) [12] [13],** **(4) XML-Dateien [20] [24]** **und die Formate signierter Daten** **(1) PAdES [27] [44] für PDF/A-Dokumente,** **(2) CAdES [26] [43] für XML, PDF/A, Text und TIFF Dokumente,**

315 [assignment: *list of objects or information types*]

(3) XAdES [25] [42] für XML-Dokumente

mit den Signaturvarianten

(1) enveloped signature,

(2) enveloping signature,

zu unterstützen.

FDP_DAU.2.2/AK.QES The TSF shall provide S_Benutzern[316] 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/AK.QES genannten Formaten sowie PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.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. [selection: *none, qualifizierter Zeitstempel über die Signatur*],

iv. bzw. wenn diese nicht vorliegen der Jetzt-Zeitpunkt;

b. das Vorhandensein des Zertifikats des VDA, der das Signaturzertifikat ausgestellt hat, in der BNetzA-VL.

c. die Korrektheit der digitalen Signatur des Signaturzertifikats,

d. die Anforderung von OCSP-Anfragen und die Auswertung von OSCP-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

316 [assignment: *list of subjects*]

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) **[assignment: *andere Form von Nachweisen*].**

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/AK.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 [76] schränkt die zu unterstützenden Kombinationen der Dokumentenfromate, Formate signierter Daten und Signaturvarianten ein. Diese Einschränkungen gelten auch für FDP_DAU.2.1/AK.QES. Die für die Prüfung der qualifizierten elektronischen Signatur notwendigen Angaben (wie z.B. Angaben zu dem der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikat) werden durch den EVG mit Hilfe der PKI-Dienste erstellt.

Die Identität des Benutzers, der den Nachweis generiert hat, wird aus dem der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikat abgeleitet. Dies kann ein Pseudonym sein.

Anwendungshinweis 161: Für die Prüfung der Zertifikate, die OSCP-Antworten und die OCSP-Zertifikate ist mindestens sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) zu unterstützen.

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: Wenn ein Konnektor die Signaturvariante „detached signature“ anbietet (etwa für weitere Fachmodule), dann sollte („should“) der ST-Autor diese Variante in FDP_DAU.2.1/AK.QES aufnehmen.

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[317] **durch nicht-qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der Chipkarten**. **Es sind die Dokumentenformate zu signierender Daten**

(1) Text-Dateien (UTF-8 [41] oder ISO-8859-15 [11]),

(2) TIFF-Dateien[40],

(3) Adobe Portable Document Format (PDF/A) [12],

(4) XML-Dateien [20] [24],

(5) MIME [34],

(6) Binärdokument,

und die Formate signierter Daten

(1) PAdES [27] [44] für PDF/A-Dokumente,

(2) CAdES [26] [43] für Text, TIFF, Adobe Portable Document Format (PDF/A) und XML Dokumente sowie Binärdokumente,

(3) S/MIME [34],

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*[318] 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/AK.Sig genannten Formaten sowie 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 OSCP-Antworten,

317 [assignment: *list of objects or information types*]

318 [assignment: *list of subjects*]

[assignment: *andere Form von Nachweisen*].

Anwendungshinweis 164: Der EVG soll die Erzeugung und die Prüfung von nicht-qualifizierten elektronischen Signaturen unterstützen. 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. Für die definierte Zuweisung muss der Autor von Sicherheitsvorgaben weitere geeignete Nachweise bringen. Zum Nachweis der erfolgreichen Prüfung müssen die für die Gültigkeitsprüfung benutzten OCSP-Antworten mit einem Zeitstempel versehen und dem Nutzer zugänglich gemacht werden. Die für FDP_DAU.2/AK.**Sig** zusätzlich unterstützten Signaturrichtlinien sind durch die Sicherheitsvorgaben zu beschreiben.

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: Für die Prüfung der Zertifikate, die OSCP-Antworten und die OCSP-Zertifikate ist mindestens sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) zu unterstützen.

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[319]**.**
FDP_DAU.2.2/AK**.**Cert	The TSF shall provide *S_Benutzern*[320] 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 OSCP-Antworten,** **(9) die Anforderung von CRL-Anfragen und die Auswertung von CRL,**

319 [assignment: *list of objects or information types*]

320 [assignment: *list of subjects*]

(10) [assignment: *andere Form von Nachweisen*].

Anwendungshinweis 167: Die Informationen aus dem OCSP-Dienst können eine gewisse Zeit in einem Cache gepuffert und verwendet werden. Dabei ist zu beachten, dass der verwendete Zeitpunkt der aus dem Cache entnommenen Prüfergebnisse nicht älter ist als der zu prüfende Signaturerstellungszeitpunkt. Der maximale Zeitraum der Verwendung des OCSP Cache kann vom Administrator vorgegeben werden.

Anwendungshinweis 168: Für die Prüfung der Zertifikate, die OSCP-Antworten und die OCSP-Zertifikate ist mindestens sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) zu unterstützen.

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[321] 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,

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

(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

.[322]

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[323] to provide restrictive[324] 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[325] 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 Schutzprofil 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[326] on all objects, based on the following attributes: [assignment: *user data attributes*].
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) [assignment: *weitere auszuführende Aktion*] [327].

322 [assignment: *additional importation control rules*]

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

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

325 [assignment: *the authorised identified roles*]

326 [assignment: *integrity errors*]

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.1 ist so zu wählen, 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. Dies kann z. B. durch eine Berechnung eines Hashwertes über die empfangenen zu signierenden Daten und eines Hashwertes über die Daten, auf die sich zu berechnende digitale Signatur, erfolgen.

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[328] to restrict the ability to (1) Modify[329] the security attribute Autorisierungsstatus zu signierender Daten, [330] **(2) Select[331] the security attribute gültige Signaturrichtlinie für zu signierende Daten, [332]** **(3) Modify[333] the security attributes angegebener Zeitpunkt signierter Daten für die Signaturprüfung[334]** to S_Benutzer_Clientsystem[335].

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

327 [assignment: *action to be taken*]

328 [assignment: *access control SFP(s), information flow control SFP(s)*]

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

330 [assignment: *list of security attributes*]

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

332 [assignment: *list of security attributes*]

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

334 [assignment: *list of security attributes*]

335 [assignment: *the authorised identified roles*]

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[336] 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[337].

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.

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

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

Dependencies:	No dependencies.
FTA_TAB.1.1/AK**.**SP	~~**Before establishing a user session**~~ **Bei Feststellung ungültig erzeugter Signaturen,** the TSF shall display an advisorywarning message regarding unauthorised use of the TOE **to S_Benutzer_Clientsystem via the standard interface**.

Anwendungshinweis 174: Die Verfeinerung des Elements FTA_TAB.1/AK**.SP** warnt den Benutzer bei festgestellten Fehlern des Signaturprozesses, wenn ungültig signierte Dateien festgestellt wurden über die Standard-Schnittstelle des Clientsystems. Die Bedingungen für ungültig signierte Dateien sind in FMT_MSA.4/AK festgelegt

6.3.3.5. Software-Update

FDP_ACC.1/AK.Update	**Subset access control / Update**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK**.**Update	The TSF shall enforce the Update-SFP[338] on subjects: (1) S_Administrator, (2) S_AK, (3) S_NK; objects: (1) Update-Pakete; operations: (1) Importieren (2) Verwenden ,[339]

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-	Das Installieren (Verwenden) des Updates kann automatisch erfolgen.

338 [assignment: *access control SFP*]

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

	Kartenterminal) verwendet.	

Tabelle 20: Operationen für Software-Update

FDP_ACF.1/AK.Update	**Security attribute based access control / Update**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/AK**.**Update	The TSF shall enforce the Update-SFP [340] to objects based on the following: subjects: (1) S_Administrator (2) S_AK, (3) S_NK objects: (1) Update-Pakete with security attributes: a. Signatur, b. Zulässige Software-Versionen .
FDP_ACF.1.2/AK**.**Update	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) Das Subjekt S_AK oder S_NK darf nur Update-Pakete importieren, deren Signatur erfolgreich geprüft wurde. (2) Die Subjekte S_Administrator, S_AK und S_NK dürfen nur Update-Pakete verwenden, die einer Firmwaregruppe angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist. .[341]
FDP_ACF.1.3/AK**.**Update	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
FDP_ACF.1.4/AK**.**Update	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. S_AK und S_NK dürfen Update-Pakete nicht automatisch anwenden, wenn die automatische Aktualisierung der Firmware durch S_Administrator deaktiviert wurde.

340 [assignment: *access control SFP*]

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

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

.[342]

Anwendungshinweis 175: Die Liste der zulässigen Software-Versionen wird in der Spezifikation *Übergreifende Spezifikation: Operations und Maintenance* [gemSpec_OM mit "Firmware-Gruppe" bezeichnet [86]. Diese muss als versionierte Liste zulässiger Firmware-Versionen für Software-Updates in jede Konnektor-Software integriert werden.

FDP_UIT.1/AK.Update	**Data exchange integrity / Update**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1/AK**.**Update	The TSF shall enforce the Update-SFP[343] to receive[344] user data ~~**in a manner**~~ protected from modification, deletion, insertion[345] errors.
FDP_UIT.1.2/AK**.**Update	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion[346] has occurred.

6.3.3.6. Verschlüsselungsdienst

FDP_ACC.1/AK.Enc	**Subset access control / Verschlüsselung**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK**.**Enc	The TSF shall enforce the Verschlüsselung-SFP[347] on subjects: (1) S_AK, (2) S_Verschlüsselungsdienst; objects:

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

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

344 [selection: *transmit, receive*]

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

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

347 [assignment: *access control SFP*]

(1) Zu verschlüsselnde Daten,
(2) Verschlüsselte Daten,
(3) Zu entschlüsselnde Daten,
(4) Entschlüsselte Daten;
operations:
(1) Verschlüsseln,
(2) Entschlüsseln,
(3) Festlegen der vorgesehenen Empfänger[348].

Operation	Beschreibung	Anmerkung
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 21: 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 [349] to objects based on the following: subjects: (1) S_AK, (2) S_Verschlüsselungsdienst; objects:

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

349 [assignment: *access control SFP*]

(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

.[350]

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 S_Verschlüsselungsdienst mit der Objekt-ID, der Identität der Verschlüsselungsrichtlinie und der Identität der vorgeschlagenen Empfängern übergeben.
(2) Das Subjekt S_Verschlüsselungsdienst darf nur ordnungsgemäß verschlüsselte Daten oder Statusmeldungen an das Subjekt S_AK zurückgeben.
(3) Das Subjekt S_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 S_Verschlüsselungsdienst nur mit Identität eines vorgesehenen Empfängers, dessen Chipkarte für die Entschlüsselung benutzt werden soll, und der Identität der zum Entschlüsseln zu verwendenden Verschlüsselungsrichtlinie übergeben.
(5) Das Subjekt S_Verschlüsselungsdienst darf nur dann die verschlüsselten Daten automatisch für die identifizierten vorgesehenen Empfänger entschlüsseln und die entschlüsselten

[350] [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*]

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.

.[351]

FDP_ACF.1.3/AK.Enc The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/AK.Enc The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Anwendungshinweis 176: Die Sicherheitsvorgaben müssen die offenen Operationen ausführen. Alle Verschlüsselungsrichtlinie für Konnektoren erlauben das automatische Verschlüsseln und Entschlüsseln von Daten. Die zum Entschlüsseln zu verwendende Chipkarte hängt von dem identifizierten vorgesehenen Empfänger und der auszuführenden Anwenungen ab.

FDP_ITC.2/AK.Enc	**Import of user data with security attributes / Verschlüsselungsdienst**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/AK.Enc	The TSF shall enforce the Verschüsselungs-SFP[352] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/AK.Enc	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/AK.Enc	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

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

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

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

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

(1) Die TSF importiert zu verschlüsselnde Daten mit dem Sicherheitsattribut „Verschlüsselungsrichtlinie“ nur für die identifizierten Fachanwendungen bzw. Anwendungsfälle und implementierten Verschlüsselungsrichtlinien.

(2) Die TSF importiert Verschlüsselungszertifikate und zu verschlüsselnde Daten mit dem Sicherheitsattribut „vorgeschlagene Empfänger“ nur nach erfolgreicher Prüfung der Gültigkeit der Verschlüsselungszertifikate der vorgesehenen Empfänger.

(3) Die TSF importiert TI-fremde X.509 CA-Zertifikate durch den Administrator über die Management-Schnittstelle

.[353]

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 mittels OCSP-Abfrage),
- oder seine Integrität durch eine Zertifikatskette bis zu einer Instanz aus der Liste der TI-fremden CA-Zertifikate für die hybride Verschlüsselung (CERT_IMPORTED_CA_LIST) mit als authentisch bekannten öffentlichen Schlüssel erfolgreich geprüft wurde.

FDP_ETC.2/AK.Enc Export of user data with security attributes / Verschlüsselungsdienst

Hierarchical to: No other components.

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

FDP_ETC.2.1/AK.Enc The TSF shall enforce the Verschüsselungs-SFP[354] 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.

353 [assignment: *additional importation control rules*]

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

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

.[355]

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.

FDP_ACC.1/AK.TLS	**Subset access control / TLS-Kanäle**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AK.TLS	The TSF shall enforce the AK-TLS-SFP[356] 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

355 [assignment: *additional exportation control rules*]

356 [assignment: *access control SFP*]

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
[357].

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. S_Fachdienst nutzt stets das X.509 Zertifikat C.FD.TLS-S für die Server-Authentisierung.	Algorithmen und Schlüssel für die Kanalverschlüsselung werden mit dem Kommunikationspartner ausgehandelt. Dem TLS-Kanal wird ein TLSConnectionIdentifier zugeordnet.

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

Operation	Beschreibung	Anmerkung
	(3) Bei der Kommunikation des EVG mit S_Clientsystem muss der Konnektor als TLS-Server die Authentifizierung des Clientsystems mit den Verfahren Basic Authentication (Username/ Password) [RFC2617] über http/TLS [RFC2818] und zertifikatsbasierte Client-Authentifizierung (X.509) [gemSpec_PKI#8.3.1.4] über TLS anbieten (vergl. [76], 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.	
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	Die beim Kanal-Aufbau

Operation	Beschreibung	Anmerkung
	entschlüsselt und integritätsgeprüft. Es werden unverfälscht empfangene Daten ausgegeben.	ausgehandelten Algorithmen und Sitzungs-Schlüssel werden verwendet.

Tabelle 22: 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[358] 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" .[359]
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.

358 [assignment: *access control SFP*]

359 [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*]

(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) [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[360].

FDP_ACF.1.3/AK.TLS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/AK.TLS The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Wenn MGM_LU_ONLINE = "Disabled", DARF der Basisdienst TLS-Dienst nach dem Bootup NICHT TLS-Kanäle zur Verfügung stellen.

(2) Der Intermediär VSDM kann die Nutzung der SessionID zur Wiederaufnahme der TLS-Verbindung ablehnen und den Aufbau einer TLS-Verbindung verlangen.

(3) Wenn MGM_LU_ONLINE = "Disabled" oder MGM_LOGICAL_SEPARATION=Enabled, DARF die Verzeichnisverwaltung NICHT TLS-Kanäle zum VZD zur Verfügung stellen.

(4) The TSF shall perform den Kanal zum VZD 15 Minuten nach der letzten vom VZD empfangenen oder von der Verzeichnisverwaltung des EVG gesendeten Daten abbauen.

(5) [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]

[361].

Anwendungshinweis 178: Für den Fall, dass durch die Konfiguration *ANCL_TLS_MANDATORY=Disabled* eine erzwungene Authentisierung der Clientsysteme abgeschaltet wurde, muss dafür gesorgt werden, dass der Nutzer über diesen Systemzustand und dessen Folgen informiert ist. Das kann beispielsweise durch eine Klarstellung im Benutzerhandbuch erfolgen. [74] bestimmt in GS-A_5322, dass der EVG im Rahmen von TLS-Session-Resumption mittels SessionID (vgl. [RFC-5246, Abschnitt 7.4.1.2]) nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) sowie damit verbundene SessionIDs sicher gelöscht werden. Das Fachmodul VSDM und der Intermediär VSDM müssen für die Verbindung zwischen Fachmodul und Intermediär TLS Session Resumption mittels Session-ID gemäß RFC 5246 nutzen, um für den wiederholten Aufbau von TLS-Verbindungen die bereits ausgehandelten Session-Parameter zu nutzen.

Anwendungshinweis 179: Der Konnektor muss beim TLS-Verbindungsaufbau den OCSP-Status des TLS-Serverzertifikates gemäß TIP1-A_7254 [76] beachten.

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

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

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[362] to restrict the ability to change_default, query, modify, delete, [assignment: other operations][363] the security attributes [assignment: ***Authentisierungsmechanismus***, *list of* ***additional*** *security attributes*][364] to S_Administrator[365]. **Änderungen der Konfiguration müssen unmittelbar durchgesetzt werden.**

Anwendungshinweis 180: Die in FMT_MSA.1/AK.**TLS** definierte Verfeinerung bezieht sich insbesondere auf solche Konfigurationen, die die Art der akzeptierten Authentisierungsmechanismen betreffen, etwa ANCL_CAUT_MODE [76]. 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[366] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]]* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AK.TLS	The TSF shall allow the S_Administrator[367] 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

362 [assignment: *access control SFP(s), information flow control SFP(s)*]

363 [selection: *change_default, query, modify, delete, [assignment: other operations]*], d.h.: die Auswahl wurde vorgenommen (alle 4 vordefinierten Werte wurden ausgewählt, außerdem wurde die Möglichkeit, andere Optionen zuzuweisen, ebenfalls zugelassen)

364 [assignment: *list of security attributes*]

365 [assignment: *the authorised identified roles*]

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

367 [assignment: *the authorised identified roles*]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/AK**.**FD	The TSF shall provide a communication channel between itself and **a S_Fachdienst** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_Fachdienst mit dem Zertifikat C.FD.TLS-S gegenüber dem EVG und EVG mit dem Zertifikat C.HCI.AUT gegenüber S_Fachdienst wenn von S_Fachmodul gefordert** ~~its end points~~ and protection of the channel data from modification **and ~~or~~** disclosure.
FTP_ITC.1.2/AK**.**FD	The TSF shall permit the TSF[368] 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[369]

Anwendungshinweis 181: Die Verfeinerung des Elementes FTP_ITC.1/AK.FD konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „Fachdienst“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem Fachdienst auf, wobei die Authentisierung der Endpunkte je nach Aufruf durch das Fachmodul beidseitig ist oder auf den Fachdienst eingeschränkt wird.

FTP_ITC.1/AK.VZD	**Inter-TSF trusted channel / Zum zentralen Verzeichnisdienst**
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[370] 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“[371].

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

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

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

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

Anwendungshinweis 182: Die Verfeinerung des Elementes FTP_ITC.1/AK.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.AK.Fachdienste können nur vertrauenswürdige Entitäten auf den VZD zugreifen.

FTP_ITC.1/AK.KSR	**Inter-TSF trusted channel / Zum KSR (Update-Server)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/AK**.**KSR	The TSF shall provide a communication channel between itself and **S_KSR** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_KSR mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and** ~~**or**~~ disclosure.
FTP_ITC.1.2/AK**.**KSR	The TSF shall permit the TSF[372] to initiate communication via the trusted channel.
FTP_ITC.1.3/AK**.**KSR	The TSF shall initiate communication via the trusted channel for Prüfung auf neue Firmware-Update-Pakete und Download neuer Firmware-Update-Pakete[373].

Anwendungshinweis 183: Die Verfeinerung des Elementes FTP_ITC.1/KSR konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „KSR“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem KSR (Update-Server) auf, wobei die Authentisierung der Endpunkte auf den KSR eingeschränkt wird.

FTP_ITC.1/AK.TSL	**Inter-TSF trusted channel / Zum TSL-Dienst**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/AK**.**TSL	The TSF shall provide a communication channel between itself and **S_TSL_Dienst** ~~another trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of **S_TSL_Dienst mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG** ~~its end points~~ and protection of the channel data from modification **and** ~~**or**~~ disclosure.
FTP_ITC.1.2/AK**.**TSL	The TSF shall permit the TSF[374] to initiate communication via the trusted channel.
FTP_ITC.1.3/AK**.**TSL	The TSF shall initiate communication via the trusted channel for

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

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

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

Download des BNetzA-VL Hashwerts und Download der BNetzA-VL[375].

Anwendungshinweis 184: Die Verfeinerung des Elementes FTP_ITC.1/TSL konkretisiert das vertrauenswürdige Produkt. Die allgemeine Formulierung „einem anderen vertrauenswürdigen IT-Produkt“ wurde durch „TSL-Dienst“ verfeinert. Die TSF baut vertrauenswürdige Kanäle zu dem TSL-Dienst auf, wobei die Authentisierung der Endpunkte auf den TSL-Dienst eingeschränkt wird.

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[376] 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*[377] **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. [76], 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.

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

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

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

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[378] **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[379].

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[380] on subjects: (1) S_AK, (2) S_Fachmodul, (3) S_Administrator objects: (1) Schlüssel für sicheren Datenspeicher,

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

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

380 [assignment: *access control SFP*]

(2) Datenobjekte des sicheren Datenspeichers,
operations:
(1) lesen
(2) schreiben
.[381]

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 23: Operationen zum Zugriff auf den sichern 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[382] 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

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

382 [assignment: *access control SFP*]

Administratorobjekt.[383]

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 „Adminstratorobjekt“ darf nur innerhalb einer Administratorsitzung entschlüsselt und gelesen und verschlüsselt und geschrieben werden, aber nicht außerhalb der Administratorsitzung gespeichert werden,

(5) [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].[384]

FDP_ACF.1.3/AK.SDS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/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) [assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*]. [385]

383 [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*]

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

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

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.

Anwendungshinweis 188: Der Autor des STs soll darstellen, wie der Inhalt des sicheren Datenspeichers bei ausgeschaltetem Konnektor geschützt ist und wie die Initialisierung des sicheren Datenspeichers erfolgt.

Anwendungshinweis 189: Die Einschränkung des Zugriffs auf Datenobjekte im Administratorbereich des sicheren Datenspeichers darf nicht nur durch entsprechende Zugriffsrechte, sondern soll durch kryptographische Mechanismen durchgesetzt werden

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[386] on subjects: (1) S_AK, (2) S_VSDM_Fachmodul, (3) S_VSDM_Intermediär, (4) S_VSDD_Fachdienst, (5) S_CMS, (6) S_eGK, (7) S_Administrator; objecte: (1) Daten der Chipkarten (Versichertenstammdaten), (2) Objektsystem der Chipkarte (eGK); operations: (1) Lesen der Versichertenstammdaten, (2) Schreiben der Versichertenstammdaten, (3) Ergänzen des Objektsystems .[387]

Operation	Beschreibung	Anmerkung
Lesen der	Lesen der	Diese Operation kann die

386 [assignment: *access control SFP*]

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

Versichertenstammdaten	Versicherten-stammdaten der eGK	Kartenkommandos SELECT, SEARCH BINARY, READ BINARY, SEARCH RECORD, READ RECORD erfordern
Schreiben der Versichertenstammdaten	Schreiben oder Modifizieren 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 24: 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[388] 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) .[389]

388 [assignment: *access control SFP*]

389 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2/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) [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

.[390]

FDP_ACF.1.3/AK**.**VSDM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/AK**.**VSDM The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

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[391] to restrict the ability to [selection: ***create,*** *change_default, query, modify,*

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

391 [assignment: *access control SFP(s), information flow control SFP(s)*]

delete, [assignment: other operations]][392] the security attributes [assignment: list of security attributes] to S_Administrator.[393]

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[394] to provide restrictive[395] 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[396] to specify alternative initial values to override the default values when an object or information is created.

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,

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

393 [assignment: *the authorised identified roles*]

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

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

396 [assignment: *the authorised identified roles*]

(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 „Ordnungsgemäss verschlüsselt“ verschlüsselter Daten nur dann auf „ordnungsgemäß“, wenn

(d) die identifizierte Verschlüsselungsrichtlinie für die zu verschlüsselnden Daten gültig ist,

(e) zu den vorgesehenen Empfängern gültige Verschlüs-

selungszertifikate existieren und für die Verschlüsselung des symmetrischen Schlüssels verwendet wurden,

(f) die durch den Xpath-Ausdruck selektierten zu verschlüsselnden Daten vollständig verschlüsselt wurden und

(g) keine Fehler auftraten.

.[397]

Anwendungshinweis 191: Die Zuweisung in der Regel (5) muss in Übereinstimmung mit den Zugriffsregeln der qualifizierten Signaturerstellungseinheit erfolgen. Für die Stapelsignatur nach TR-03114 [67] 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 ≤ m ≤ 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 [67], Schritt 4, dadurch um, dass in den aufgeführten Fällen alle bisher erstellen Signaturen des autorisierten Stapels verworfen und der Signaturprozess abgebrochen werden muss.

Wenn der Benutzer einen Abbruch des Signaturvorganges anfordert, so werden die vorher für den autorisierten (Teil-) Signaturstapel erstellten Signaturen verworfen und gelöscht und die Erzeugung der noch ausstehenden Signaturen wird abgebrochen. Wenn bei einer erneuten Signatur-PIN-Eingabe des Stapels ein Fehler auftritt (z. B. die zulässige Zeit für die PIN-Eingabe überschritten wird oder die PIN-Eingabe falsch ist), so soll dies wie ein vom Benutzer geforderter Abbruch behandelt werden.

Die Regelungen zur Signaturerstellung in der SFR FMT_MSA.4/AK beziehen sich auf die in diesem PP beschriebenen Signaturarten. Sollen vom EVG weitere Signaturarten – bspw. Komfortsignatur – umgesetzt werden, kann in Abstimmung mit der Zertifizierungsstelle für diese Signaturarten teilweise von der SFR abgewichen werden – bspw. Regel (6)(f).

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

397 [assignment: *rules for setting the values of security attributes*]

resource is made unavailable upon the deallocation of the resource from[398] 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

.[399]

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 müssen eventuell vorhandene Puffer-Inhalte (Cache) sicher gelöscht werden.

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,

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

399 [assignment: *list of objects*]

(10) Fachmodul,
(11) Fachdienst

[400].

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

.[401]

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[402] the functions Online Kommunikation, Signaturdienst und Logische Trennung[403]to Administrator[404].

The following rules apply:

1. If the attribute MGM_LU_ONLINE is set to "Disabled",

400 [assignment: *the authorised identified roles*]

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

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

403 [assignment:*list of functions*]

404 [assignment: *the authorised identified roles*]

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/AK.Update.

2. If the attribute MGM_LU_SAK is set to "Disabled", the Signaturdienst for QES according to the chapters 6.3.1.3 and 6.3.3.4 is deactivated.

3. If the logical separation is activated (attribute MGM_LOGICAL_SEPARATION set to "Enabled"), the following rules apply:

(1) If invoked from an external interface, the Verschlüsselungsdienst of the Konnektor must not check the revocation status of certificates.

(2) If invoked from an external interface, the Signaturdienst of the Konnektor must not check the revocation status of certificates.

(3) IF MGM_LU_ONLINE is not enabled, the NTP server of the Konnektor must be deactivated.

(4) If MGM_LU_ONLINE is set to "Enabled", the Konnektor may only resolve the namespace „TI (*.DNS_TOP_LEVEL_DOMAIN_TI) " for internal services and internal Fachanwendungen and must not resolve this namespace for requests originatred from the LAN.

(5) The Konnektor must block all communication on its external interfaces with the following systems:

a. with systems in the network segment ANLW_AKTIVE_BESTANDSNETZE initiated by „Aktive Komponenten",

b. with the Internet via SIS and IAG.

Anwendungshinweis 193: Wenn MGM_LU_ONLINE=Disabled gesetzt ist, so baut der Konnektor grundsätzlich keine Online-Verbindungen zum WAN auf und beendet bestehende Kommunikation einschließlich VNP-Client, vergl. FMT_MSA.1/NK. Wenn MGM_LU_ONLINE=Enabled, aber MGM_LOGICAL_SEPARATION=Enabled, dann verhalten sich definierte Teile des Konnektors analog zu einer Auftrennung der Online-Verbindungen. Die Funktion „logische Trennung" muss nicht vom EVG umgesetzt werden. Ist die Funktion nicht vorhanden, entspricht dies der Konfiguration MGM_LOGICAL_SEPARATION = „disabled".

FMT_MTD.1/AK.Admin	**Management of TSF data / Administration**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AK.Admin	The TSF shall restrict the ability to

(1) set, query, modify and delete[405] the roles from other users[406],

(2) set, modify and delete[407] the authentication credentials for administrators[408],

(3) set and modify[409] the Arbeitsplatzkonfiguration with assigned Clientsystem and eHealth-Kartenterminals[410],

(4) set and modify[411] the Zeitpunkten und Gültigkeitsdauer der Prüfungsergebnisse zur Gültigkeit qualifizierter Zertifikate für die Erzeugung ordnungsgemäßer qualifizierten elektronischen Signaturen[412],

(5) change_default[413] of the gültigen Signaturrichtlinie für Signaturerzeugung[414],

(6) change_default[415] of the gültigen Signaturrichtlinie für Signaturprüfung[416],

(7) modify[417] the configuration parameter to activate or deactivate the automatic installation of software updates[418],

(8) import[419] the update data for Karten-Terminals and execute the update[420],

(9) configure[421] the loggable system events[422],

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

406 [assignment: *list of TSF data*]

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

408 [assignment: *list of TSF data*]

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

410 [assignment: *list of TSF data*]

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

412 [assignment: *list of TSF data*]

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

414 [assignment: *list of TSF data*]

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

416 [assignment: *list of TSF data*]

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

418 [assignment: *list of TSF data*]

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

420 [assignment: *list of TSF data*]

(10) export and import[423] the configuration data of the TOE[424],

(11) set and modify[425] the maximum lifetime of OCSP cache entries[426]

(12) set and modify[427] the keys of the sicheren Datenspeichers[428],

(13) set and import[429] the X.509 certificates of Clientsystemen[430],

(14) reset to factory settings[431] of ~~the~~ all TSF data (factory reset)[432],

(15) import[433] the CA certificates of an encryption PKI[434]

to administrator[435].

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. FDP_ITC.2/NK.TLS).

Anwendungshinweis 195: Regel (7) von FMT_MTD.1.1/AK.Admin gilt auch als erfüllt, wenn der TOE keine Funktionalität für automatische Updates besitzt.

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[436] the public keys of the CVC root CA[437] to the CMS of the gSMC-K[438],

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

422 [assignment: *list of TSF data*]

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

424 [assignment: *list of TSF data*]

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

426 [assignment: *list of TSF data*]

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

428 [assignment: *list of TSF data*]

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

430 [assignment: *list of TSF data*]

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

432 [assignment: *list of TSF data*]

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

434 [assignment: *list of TSF data*]

435 [assignment: *the authorised identified roles*]

(2) **import and permanently store[439] the public keys of the CVC root CA by the use of cross CVC[440] to S_AK[441].**

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, (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) [Selection: *Signaturrichtlinie, Verschlüsselungsrichtlinie*][442] 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 [83] muss gemäß Schalenmodell bis zu einem gültige CA-Zertifikat der ausstellenden (zugelassenen) CA, das in einer

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

437 [assignment: *list of TSF data*]

438 [assignment: the authorised identified roles]

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

440 [assignment: *list of TSF data*]

441 [assignment: the authorised identified roles]

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

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 [70] 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) [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*].[443]

when interpreting the TSF data from another trusted IT product.

Anwendungshinweis 196: Die Vertrauenswürdigkeit des IT-Produktes, von dem TSF-Daten importiert werden, ergibt sich aus einer gültigen digitalen Signatur, die mit den im EVG vorhandenen öffentlichen Schlüsseln der bekannten Vertrauensanker ggf. in einer Zertifikatskette erfolgreich geprüft werden konnte. Die „Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen“ ist gegeben, wenn (i) die Signaturrichtlinie keine qualifizierte elektronische Signatur fordert, oder (ii) die Signaturrichtlinie eine qualifizierte elektronische Signatur und die in diesem Schutzprofil für qualifizierte elektronische Signaturen definierten Regeln gemäß FDP_ACF.1/AK**.Sgen**, FDP_ACF.1/AK**.SigPr**, FDP_DAU.2/AK**.QES** und FDP_DAU.2/AK**.Cert** einhält. Die Sicherheitsvorgaben können weitere einschränkende Regeln für fortgeschrittene oder andere digitale Signaturen festlegen.

Die in der letzten Regeln 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 entsprechend FDP_ACF.1/AK**.Update**.

Anwendungshinweis 197: Die BNetzA-VL muss gemäß Anforderung A_6730 der Konnektor-Spezifikation [76] 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 [76] interpretieren.

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

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 [76]** when the following types of failures occur:

(1) according to TAB_KON_503 [76] with type „SEC“ and severity „fatal“.

(2) [assignment: list of additional types of failures in the TSF] [444].

Failures occured during the self test of the TOE (see FPT_TST.1/AK.Run-Time and FPT_TST.1/AK.Out-Of-Band) must trigger a blockage of the affected parts of the TSF.

Anwendungshinweis 198: Für dedizierte Fehlerarten muss der EVG bestimmte weitere Funktionalität unterbinden. Diese Fehlerarten und die erlaubten bzw. verbotenen Dienste sind in Tabelle TAB_KON_504 in [76] definiert.

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[445] 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.[446]

(2) bei der Meldung eines eHealth-Kartenterminals über das Stecken einer Chipkarte[447] 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. [448]

444 [assignment: *list of types of failures in the TSF*]

445 [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

446 [assignment: *List of properties of the external entities*]

447 [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

448 [assignment: *List of properties of the external entities*]

(3) bei entfernter Eingabe von PIN- oder PUK[449] 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.

.[450]

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 [assignment: *action for unknown smart cards*].[451]

Anwendungshinweis 200: Die offene Operation im Element FPT_TEE.1.2 muss in den Sicherheitsvorgaben entsprechend der Unterstützung weiterer Chipkarten ausgeführt werden. Wenn keine weiteren Chipkarten unterstützt werden, ist eine Fehlermeldung an den EVG über einen unbekannten Kartentyp zu übergeben. Die Testfolge für ein eHealth-Kartenterminal besteht in dem Aufbau eines TLS-Kanals mit Prüfung des Zertifkats einer gültigen gSMC und des Pairing-Geheimnis (s. [77]). Die Testfolge für eine KVK besteht im Lesen und Auswerten des ATR der Chipkarte. Die Testfolge für Chipkarten des Kartentyps eGK, HBA, gSMC-KT und SMC-B umfasst die sichere Bestimmung der Karte und des Kartentyps.

FPT_TST.1/AK.Run-Time	**TSF testing / Normalbetrieb**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1/AK**.**Run-Time	The TSF shall run a suite of self tests beim Anlauf und regelmäßig während des Normalbetriebs[452] to demonstrate the correct operation of [assignment: *parts of TSF*][453].

449 [selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]

450 [assignment: *list of properties of the external entities*]

451 [assignment: *action(s)*]

452 [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]*]

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

FPT_TST.1.2/AK**.**Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of [assignment: *parts of TSF data*][454].
FPT_TST.1.3/AK**.**Run-Time	The TSF shall provide authorised users with the capability to verify the integrity of [assignment: *parts of TSF*][455].

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. Know-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** soll dem Autor der Sicherheitsvorgaben einfache Möglichkeiten zur Präzisierung geben. Die Zuweisung darf nicht leer sein.

FPT_TST.1/AK.Out-Of-Band	**TSF testing / Out-Of-Band**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1/AK**.**Out-Of-Band	The TSF shall run a suite of self tests **durch TSF-Komponenten mit integritätsgeschützt gespeichertem Code** beim Erstanlauf und auf Anforderung eines autorisierten Benutzers[456] to demonstrate the correct operation of TSF[457].
FPT_TST.1.2/AK**.**Out-Of-Band	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[458].
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 **[assignment: *parts of TSF mit gespeichertem ausführbarem TSF-Code*]**[459].

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

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

[456] [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]*]

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

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

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

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. Eine mögliche Testmethode könnte darin bestehen, dass die Integrität des ausführbaren Code und der TSF-Daten durch eine gesonderte Software getestet wird, die nicht auf dem EVG gespeichert ist, und deren Integrität nicht durch die Funktionsstörungen oder Angriffe, die zu Verfälschungen geführt haben könnten, beeinträchtigt ist. Auf dem Konnektor könnten geschützte Speicherbereiche und Testmechanismen implementiert sein, die ggf. sowohl bei Erstanlauf als auch bei Anlauf genutzt werden. Die Verfeinerungen der Elemente FPT_TST.1/AK.**Out-Of-Band** soll dem Autor der Sicherheitsvorgaben einfache Möglichkeiten zur Erweiterung geben. Die Zuweisung kann auch leer sein.

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 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 [selection, choose one of: *minimum,*

basic, detailed, not specified] level of audit; and

c) The following specified security-relevant auditable events:

- *Power on / Shut down (einschließlich der Art der ausgelösten Aktion, z. B. Reboot) des Anwendungskonnektors,*
- *Durchführung von Softwareupdates einschließlich nicht erfolgreicher Versuche des Anwendungskonnektors,*
- *Zeitpunkt von Änderungen der Konfigurationseinstellungen und Export/Import von Konfigurationsdaten des Anwendungskonnektors,*
- *kritische Betriebszustände wie in der Tabelle in FPT_FLS.1/AK aufgelistet des Anwendungskonnektors,*
- *Ereignisse vom Typ „Sec" des Anwendungskonnektors,*
- *[assignment: additional events]*

[460].

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

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

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

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 [76] gibt im Anhang F eine Übersicht der Ereignisse (Events), wobei nur die Beschreibungen der Ereignisse 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 [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] 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.

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

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[461] unauthorised modifications to the stored audit records in the audit trail.

Anwendungshinweis 204: Nach [76] 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[462] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

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

462 [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

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. 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 [76],**
>
> **(2) der Vertraulichkeit und der Integrität der TSF-Daten (s. TIP1-A_4813 Persistieren der Konfigurationsdaten [76]),**
>
> **(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 [76], 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.

6.5. 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

SFR	Abhängig von	Erfüllt durch
		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
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	FDP_ITC.2/AK.Enc FCS_CKM.4/AK

SFR	Abhängig von	Erfüllt durch
	Sicherheitsattribute oder FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen oder FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	
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	FCS_CKM.1/AK.AES FCS_CKM.4/AK, asymmetrische Operationen in den Chipkarten

SFR	Abhängig von	Erfüllt durch
	Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	
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 Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	FDP_ITC.2/AK.Sig, FCS_COP.1/AK.SHA verwendet keine Schlüssel.
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.PKCS.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 Schlüsselvernich-tung da Signaturprüfung
FCS_COP.1/AK.SigVer.P	[FDP_ITC.1 Import von Benutzerdaten ohne	FDP_ITC.2/AK.Sig

SFR	Abhängig von	Erfüllt durch
SS	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
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.
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.4/AK Beachte, die Schlüssel für die Signaturerzeugung sind in den Chipkarten implementiert. Deshalb wird

SFR	Abhängig von	Erfüllt durch
	FCS_CKM.1 Kryptographische Schlüsselgenerierung] FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	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

SFR	Abhängig von	Erfüllt durch
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/AK.Update	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	FDP_ACF.1/AK.Update
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 Sicherheits-attribute werden gemäß FDP_ITC.2/AK.Enc importiert und nicht über initiale Vorzugswerte vergeben.
FDP_ACF.1/AK.Infomod	FDP_ACC.1 Teilweise Zugriffskontrolle	FDP_ACC.1/AK.Infomod FMT_MSA.3/AK.Infomod

SFR	Abhängig von	Erfüllt durch
	FMT_MSA.3 Initialisierung statischer Attribute	
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 Sicherheits-attribute werden durch die Authentisierung der Chip-karten 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 Sicherheits-attribute 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.
FDP_ACF.1/AK.Update	FDP_ACC.1 Teilweise Zugriffskontrolle FMT_MSA.3 Initialisierung statischer Attribute	FDP_ACC.1/AK.Update Es findet keine Initialisierung der Sicherheitsattribute für

SFR	Abhängig von	Erfüllt durch
		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 Sicherheits-attribute durch geprüfte digitale Signaturen gesichert

SFR	Abhängig von	Erfüllt durch
		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	-
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/AK.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/AK.Update, FTP_ITC.1/AK.KSR, FTP_ITC.1/AK.TSL, 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	FIA_UID.1/AK

SFR	Abhängig von	Erfüllt durch
	Identifikation	
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
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	FMT_MSA.1/AK.TLS

SFR	Abhängig von	Erfüllt durch
	Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	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	-
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	-

SFR	Abhängig von	Erfüllt durch
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 25: Erfüllung der Abhängigkeiten der funktionalen Sicherheitsanforderungen

6.5.3. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors durch SFRs des Netzkonnektors

Tabelle 26 stellt die Abbildung der Sicherheitsziele des Netzkonnektors auf Sicherheitsanforderungen des Konnektors zunächst tabellarisch im Überblick dar. In Abschnitt 6.5.5 wird die Abbildung erläutert und die Erfüllung der Sicherheitsziele durch die Anforderungen begründet.

Sicherheitsanforderung an den EVG	O.NK.TLS_**Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FTP_ITC.1/NK.VPN_TI							X		X	X			
FTP_ITC.1/NK.VPN_SIS							X		X	X			
FDP_IFC.1/NK.PF											X	X	X
FDP_IFF.1/NK.PF											X	X	X
FMT_MSA.3/NK.PF											X	X	
FPT_STM.1/NK					X	X							
FPT_TDC.1/NK.Zert								X					
FDP_RIP.1/NK		X											
FPT_TST.1/NK		X											
FPT_EMS.1/NK		X							X	X			
FAU_GEN.1/NK.SecLog					X								
FAU_GEN.2/NK.SecLog					X								
FMT_SMR.1./NK	X			X							X	X	
FMT_MTD.1/NK				X									
FIA_UID.1/NK.SMR				X									
FTP_TRP.1/NK.Admin	X			X									
FMT_SMF.1/NK	X			X							X	X	
FMT_MSA.1/NK.PF				X							X	X	
FMT_MSA.4/NK				X									
FCS_COP.1/NK.Hash		X								X			
FCS_COP.1/NK.HMAC										X			
FCS_COP.1/NK.Auth			X				X						

Sicherheitsanforderung an den EVG	O.NK.TLS_**Krypto**	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
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 26: Abbildung der EVG-Ziele auf Sicherheitsanforderungen

6.5.4. Überblick der Abdeckung von Sicherheitszielen des Konnektors durch SFRs des Netzkonnektors und des Anwendungskonnektors

Funktionale Sicherheits-anforderung (SFR)	O.AK.Basis_Krypto	O.AK.Admin	O.AK.IFD-Komm	O.AK.Chipkartendienst	O.AK.EVG_Modifikation	O.AK.VAD	O.AK.Enc	O.AK.Dec	O.AK.Sig.exklusivZugriff	O.AK.Sig.SignQES	O.AK.Sig.SignNonQES	O.AK.Sig.Einfachsignatur	O.AK.Sig.Stapelsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FCS_CKM.1/NK.TLS	X		X															X									
FCS_COP.1/NK.TLS.HMAC	X		X															X	X								
FCS_COP.1/NK.TLS.AES	X		X															X	X								
FCS_COP.1/NK.TLS.Auth	X		X															X	X								
FCS_CKM.1/NK.Zert																		X									

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.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FDP_ETC.2/NK.TLS																		X									
FDP_ITC.2/NK.TLS																		X									
FTP_TRP.1/NK.Admin																						X					
FAU_GEN.1/AK		X																		X							
FAU_SAR.1/AK		X																		X							
FAU_STG.1/AK		X																		X							
FAU_STG.4/AK		X																		X							
FCS_CKM.1/AK.AES	X		X				X																				
FCS_CKM.4/AK	X		X				X	X																			
FCS_COP.1/AK.AES	X		X				X	X										X	X								
FCS_COP.1/AK.CMS.Ent	X							X																			
FCS_COP.1/AK.CMS.SigPr	X															X											
FCS_COP.1/AK.CMS.Sign	X									X	X																
FCS_COP.1/AK.CMS.Ver	X						X																				
FCS_COP.1/AK.PDF.SigPr	X															X											
FCS_COP.1/AK.PDF.Sign	X									X	X																
FCS_COP.1/AK.PKCS.SigPr	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																				

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.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FDP_ACC.1/AK.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														
FDP_ACC.1/AK.SigPr														X	X	X											
FDP_ACC.1/AK.TLS																		X	X							X	X
FDP_ACC.1/AK.SDS		X																									
FDP_ACC.1/AK.Update																						X					
FDP_ACC.1/AK.VSDM																										X	
FDP_ACF.1/AK.eHKT			X																								
FDP_ACF.1/AK.Enc							X	X																			
FDP_ACF.1/AK.Infomod																							X		X		
FDP_ACF.1/AK.KD				X																			X				
FDP_ACF.1/AK.PIN				X		X																		X			
FDP_ACF.1/AK.Sgen									X	X	X	X	X														
FDP_ACF.1/AK.SigPr														X	X	X											
FDP_ACF.1/AK.TLS																		X	X							X	X
FDP_ACF.1/AK.SDS		X																									
FDP_ACF.1/AK.Update																						X					
FDP_ACF.1/AK.VSDM																										X	
FDP_DAU.2/AK.Cert										X				X	X	X											
FDP_DAU.2/AK.QES										X				X	X	X											
FDP_DAU.2/AK.Sig											X			X	X	X											
FDP_ETC.2/AK.Enc							X	X																			
FDP_ITC.2/AK.Enc							X	X																			
FDP_ITC.2/AK.Sig										X																	
FDP_RIP.1/AK			X		X		X	X	X																		
FDP_SDI.2/AK									X																		
FDP_UCT.1/AK.TLS			X																								

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.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
FDP_UIT.1/AK.TLS			X																								
FDP_UIT.1/AK.Update																						X					
FIA_API.1/AK													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														
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														
FMT_MOF.1/AK		X																									
FMT_MSA.1/AK.User									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																					

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.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Selbsttest	O.AK.LAN	O.AK.WAN	O.AK.Protokoll	O.AK.Zeit	O.AK.Update	O.AK.exklusivZugriff	O.AK.PinManagement	O.AK.Infomodell	O.AK.VSDM	O.AK.VZD
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														
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														
FTP_ITC.1/AK.VZD																											X
FTP_ITC.1/AK.KSR																						X					
FTP_ITC.1/AK.TSL																						X					

Tabelle 27: Abdeckung der Sicherheitsziele des EVG durch Sicherheitsanforderungen

6.5.5. Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors

In diesem Abschnitt wird erklärt, warum die Kombination der individuellen funktionalen Sicherheitsanforderungen (SFR) des Netzkonnektors gemeinsam die formulierten Sicherheitsziele erfüllt.

Dazu wird in der folgenden Tabelle 28 jedes EVG-Ziel in einzelne Teilaspekte zerlegt, die dann auf Sicherheitsanforderungen abgebildet werden.[463] Um die Abbildung zu erklären (im Sinne des von Common Criteria geforderten Erklärungsteils / Rationale), wird in der Tabelle zu jeder solchen Abbildung eines Aspekts in der folgenden Zeile eine Begründung gegeben. Die Begründung zitiert, wo dies möglich ist, Sätze aus dem entsprechenden EVG-Ziel. Solche Zitate sind durch Anführungszeichen und Kursivschrift gekennzeichnet.

Grundsätzlich gilt, dass die korrekte Umsetzung eines Ziel in Sicherheitsanforderungen durch die im CC Teil 2 [2] aufgeführten Abhängigkeiten zwischen funktionalen Sicherheits-anforderungen (SFRs) unterstützt wird: Häufig lässt sich leicht ein SFR finden, welches wesentliche Aspekte des EVG-Ziels umsetzt. Betrachtet man alle Abhängigkeiten, so ergibt

463 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

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 FDP_ACF.1/AK.TLS
	Begründung: Für die Einrichtung einer sicheren TLS-Verbindung zwischen Konnektor und Clientsystemen ermöglicht der EVG das Exportieren von X.509 Zertifikaten für Clientsysteme und die zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle entsprechend FDP_ETC.2/NK.TLS (FDP_ACF.1/AK.TLS erfüllt die Zugriffskontrolle dafür). 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 (FDP_ACF.1/AK.TLS erfüllt die Zugriffskontrolle dafür) über die gesicherte Management-Schnittstelle durch den Administrator importiert werden (FTP_TRP.1/NK.Admin), um ggf. benötigte Betriebszustände wiederherzustellen. Die importierten Zertifikate werden nach den Vorgaben in FPT_TDC.1/NK.TLS.Zert interpretiert. Dabei wird auch eine	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	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 [68] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [74]*“ 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*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	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 Intergritätsprüfungen werden Hashwerte wie von FCS_COP.1/NK.Hash gefordert verwendet. Dieses SFR hat die formalen Abhängigkeiten FCS_CKM.4/NK und FCS_CKM.1/NK, wobei FCS_CKM.4/NK nicht erfüllt werden muss, sofern im Rahmen der Hashwertberechnung keine geheimen Schlüssel verwendet werden. FCS_CKM.1/NK fordert, dass das Schlüsselmaterial (z. B. Integritätsprüfschlüssel) generiert wird. Anmerkung: Alternativ könnte ein Hersteller diese Schlüssel auch importieren; dazu wäre dann zusätzlich FDP_ITC.1 oder FDP_ITC.2 aufzunehmen.	
	Schutz gegen unbefugte Kenntnisnahme (Side Channel-Analysen)	FPT_EMS.1/NK
	Begründung: „*Der EVG schützt sich selbst und die ihm anvertrauten Benutzerdaten.*“ Um den Aspekt „*die ihm anvertrauten Benutzerdaten*“ vollständig abzudecken, wurde die explizite Komponente FPT_EMS.1/NK ergänzt. Dieses SFR fordert genau die Analyse, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen.	
O.NK.Stateful	dynamischer Paketfilter implementiert zustandsgesteuerte Filterung (stateful packet inspection)	FDP_IFC.1/NK.PF → FDP_IFF.1/NK.PF
	Begründung: „*Der EVG implementiert zustandsgesteuerte Filterung (stateful packet inspection) mindestens für den WAN-seitigen dynamischen Paketfilter.*“ Diese Paketfilterung wurde als Informationsflusskontrolle modelliert (FDP_IFC.1/NK.PF, FDP_IFF.1/NK.PF). Die zustandsgesteuerte Filterung wurde in den Operationen und im Refinement zu FDP_IFF.1/NK.PF modelliert.	
O.NK.EVG_Authenticity	Auslieferungsverfahren: Nur authentische EVGs können in Umlauf gebracht werden	FCS_COP.1/NK.Auth FCS_CKM.1/NK FCS_CKM.4/NK
	Begründung: „*Das Auslieferungsverfahren und die Verfahren zur Inbetriebnahme des EVGs stellen sicher, dass nur authentische EVGs in Umlauf gebracht werden können. Gefälschte EVGs müssen vom*	

<table>
<tr><th>EVG-Ziel</th><th>Aspekt des Ziels</th><th>SFR, SAR
(vgl. Abschnitt 6.2 oder 6.4)</th></tr>
<tr><td></td><td colspan="2">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.</td></tr>
<tr><td rowspan="2">O.NK.Admin_EVG</td><td>rollenbasierte Zugriffskontrolle für administrative Funktionen, Liste dieser administrativen Funktionen
Identifikation / Autorisierung des Administrators
sicherer Pfad
Beschränkung der Administration der Firewall-Regeln</td><td>FMT_MTD.1/NK
FMT_SMR.1./NK
FMT_SMF.1/NK
FIA_UID.1/NK.SMR
FMT_MSA.4/NK
FTP_TRP.1/NK.Admin
FMT_MSA.1/NK.PF</td></tr>
<tr><td colspan="2">Begründung:
„Der EVG setzt eine Zugriffskontrolle für administrative Funktionen um: Nur Administratoren dürfen administrative Funktionen ausführen.“ →
FMT_MTD.1/NK beschränkt den Zugriff wie vom Ziel gefordert auf die Rolle Administrator. FMT_SMR.1./NK modelliert als abhängige Komponente diese Rolle (Administrator). FIA_UID.1/NK.SMR erfordert eine Identifikation des Benutzers vor jeglichem Zugriff auf administrative Funktionalität. Die Menge der administrativen Funktionen wird in FMT_SMF.1/NK aufgelistet.
„Dazu ermöglicht der EVG die sichere Identifikation und Autorisierung (auf Basis einer in der IT-Umgebung durchgeführten Authentisierung) eines Administrators, welcher die lokale und/oder (optional) entfernte Administration des EVG durchführen kann.“ →
Da die Authentisierung des Administrators in der Einsatzumgebung erfolgen kann, muss der EVG die Autorisierung als Sicherheitsattribut von außen übernehmen. Die dabei anzuwendenden Regeln wurden in FMT_MSA.4/NK modelliert.
„Die Administration erfolgt rollenbasiert.“ → FMT_SMR.1./NK modelliert die Rolle Administrator.
„Weil die Administration über Netzverbindungen (lokal über PS2 oder zentral über PS3) erfolgt, sind die Vertraulichkeit und Integrität des für die Administration verwendeten Kanals sowie die Authentizität seiner Endstellen zu sichern (Administration über einen sicheren logischen Kanal).“ → FTP_TRP.1/NK.Admin fordert genau diesen sicheren logischen Kanal zum Benutzer (trusted path).</td></tr>
</table>

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	„*Der EVG verhindert die Administration folgender Firewall-Regeln: …*“ → Dieser Aspekt wird durch das Refinement zu FMT_MSA.1/NK.PF abgebildet. Schließlich unterstützt die Benutzerdokumentation (AGD_OPE.1) bei der Administration der Paketfilter-Regeln.	
O.NK.Protokoll	EVG protokolliert sicherheitsrelevante Ereignisse mit Daten und Zeitstempel	FAU_GEN.1/NK.SecLog FAU_GEN.2/NK.SecLog FPT_STM.1/NK
	Begründung: „*Der EVG protokolliert sicherheitsrelevante Ereignisse und stellt die erforderlichen Daten bereit.“* → FAU_GEN.1/NK.SecLog fordert eine Protokollierung für die in der Operation explizit aufgelisteten Ereignisse und stellt Anforderungen an den Inhalt der einzelnen Log-Einträge. FAU_GEN.2/NK.SecLog fordert, dass die Benutzeridentitäten mit protokolliert werden. FPT_STM.1/NK stellt den Zeitstempel bereit.	
O.NK.Zeitdienst	regelmäßige Zeitsynchronisation	FPT_STM.1/NK
	Begründung: „*Der EVG synchronisiert die Echtzeituhr gemäß OE.NK*.Echtzeituhr *in regelmäßigen Abständen über einen sicheren Kanal mit einem vertrauenswürdigen Zeitdienst (siehe OE.NK*.Zeitsynchro*).*“ → (Refinement zu) FPT_STM.1/NK: Synchronisation mindestens einmal innerhalb von 24 Stunden; Information, falls die Synchronisierung nicht erfolgreich durchgeführt werden konnte	
O.NK.VPN_Auth	gegenseitige Authentisierung mit VPN-Konzentrator (Telematikinfrastruktur-Netz)	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Auth → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK
	Begründung: FCS_COP.1/NK.Auth setzt direkt die Anforderung nach einer Authentisierung des EVGs gegenüber dem VPN-Konzentrator um, indem es die dazu zu verwendenden Algorithmen spezifiziert. FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS fordern die sicheren Kanäle mit gegenseitiger Authentifizierung („ … provides assured identification of its end points …“) zu den VPN-Konzentratoren in die Telematikinfrastruktur bzw. ins Internet. FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS (IPsec) und FCS_CKM.2/NK.IKE (IKE) legen fest, welche Protokolle im Rahmen des Kanalaufbaus verwendet werden sollen. Zwar geht es in	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	FCS_CKM.2/NK.IKE vorrangig um die Schlüsselableitung, diese ist aber mit der Authentisierung kombiniert. FCS_CKM.1/NK fordert, dass entsprechendes Schlüsselmaterial für die Authentisierung generiert wird (evtl. unter Rückgriff auf eine gSMC-K, welches in den EVG eingebracht wird). FCS_CKM.4/NK unterstützt als abhängige Komponente.	
O.NK.Zert_Prüf	Gültigkeitsprüfung von Zertifikaten mit Hilfe von TSL und der CRL	FPT_TDC.1/NK.Zert
	Begründung: Zertifikatsprüfung: „*Der EVG führt im Rahmen der Authentisierung eines VPN-Konzentrators eine Gültigkeitsprüfung der Zertifikate, die zum Aufbau des VPN-Tunnels verwendet werden, durch. Die zur Prüfung der Zertifikate erforderlichen Informationen werden dem Konnektor in Form einer zugehörigen CRL und einer TSL bereitgestellt.*“ FPT_TDC.1/NK.Zert fordert, dass der EVG Informationen über die Gültigkeit von Zertifikaten korrekt interpretiert. In der Zuweisung wurden TSL und CRL explizit erwähnt: „*The TSF shall provide the capability to consistently interpret information – distributed in the form of a TSL (Trust-Service Status List) or CRL (Certificate Revocation List) information …*“ Die Zertifikatsprüfung wird für VPN-Konzentratoren der Telematikinfrastruktur-Netzes bzw. des Sicheren Internet Service durchgeführt. FPT_TDC.1/NK.Zert fordert ferner explizit, dass der EVG Informationen „*about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects”*interpretiert.	
O.NK.VPN_Vertraul	Vertraulichkeit der Nutzdaten im VPN (Telematikinfrastruktur-Netz) IPsec-Kanal: Ableitung von *session keys*, AES-Verschlüsselung mit den *session keys* , Zerstörung der *session keys* nach Verwendung, Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.IPsec, → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_COP.1/NK.ESP → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Vertraulichkeit der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der Nutzdaten zwischen EVG und entfernten VPN-*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Konzentratoren verschlüsselt (vor dem Versand) bzw. entschlüsselt (nach dem Empfang) der Konnektor die Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht.“ → Die Verschlüsselung wird durch FTP_ITC.1/NK.VPN_TI (im Fall der Telematikinfrastruktur) bzw. FTP_ITC.1/NK.VPN_SIS (im Fall des Sicheren Internet Service) gefordert *(„…protection of the channel data from modification and disclosure“*, man beachte das Refinement von „or“ zu „and“). FCS_COP.1/NK.IPsec ermöglicht die Definition der zu verwendenden Verschlüsselungsalgorithmen, hier AES gemäß FCS_COP.1/NK.ESP. FCS_CKM.4/NK unterstützt als abhängige Komponente ebenfalls. Für einzelne Verbindungen werden jeweils eigene *session keys* im Rahmen des Diffie-Hellman-Keyexchange-Protocols abgeleitet. FCS_CKM.1/NK fordert eine solche Generierung von *session keys*. *„Während der gegenseitigen Authentisierung erfolgt die Aushandlung eines Session Keys.*“ → Mittels FCS_CKM.2/NK.IKE (IKE) werden die abgeleiteten Sitzungsschlüssel, die für die Verschlüsselung verwendet werden, mit der die Vertraulichkeit der Nutzdaten sichergestellt wird, mit der Gegenstelle ausgetauscht. Die Nutzdaten werden mit AES gemäß FCS_COP.1/NK.ESP verschlüsselt. FPT_EMS.1/NK sorgt dafür, dass die *session keys*, welche im Rahmen der gegenseitigen Authentisierung abgeleitet werden, auch von Angreifern mit hohem Angriffspotential nicht in Erfahrung gebracht werden können. Diese *session keys* sichern die Vertraulichkeit der nachfolgenden Kommunikation.	
O.NK.VPN_Integrität	Integrität der Nutzdaten im VPN, (Telematikinfrastruktur-Netz) Ableitung von *session keys*, Austausch der *session keys* mit Gegenstelle, Zerstörung der *session keys* nach Verwendung Integritätssicherung bei IKE und IPsec Ableitung von *session keys*, Zerstörung der *session keys* nach Verwendung Geheimhaltung der *session keys*	FTP_ITC.1/NK.VPN_TI FTP_ITC.1/NK.VPN_SIS FCS_COP.1/NK.Hash → FCS_CKM.1/NK → FCS_CKM.2/NK.IKE → FCS_CKM.4/NK FCS_COP.1/NK.HMAC → FCS_CKM.1/NK → FCS_CKM.4/NK FPT_EMS.1/NK
	Begründung: „*Der EVG schützt die Integrität der Nutzdaten bei der Übertragung von und zu den VPN-Konzentratoren. Bei der Übertragung der*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	Nutzdaten zwischen EVG und entfernten VPN-Konzentratoren sichert (vor dem Versand) bzw. prüft (nach dem Empfang) der Konnektor die Integrität der Nutzdaten; dies wird durch die Verwendung des IPsec-Protokolls erreicht." → Die Integritätssicherung wird durch FTP_ITC.1/NK.VPN_TI und FTP_ITC.1/NK.VPN_SIS gefordert („*...protection of the channel data from modification and disclosure*", man beachte das Refinement von „or" zu „and"). FCS_COP.1/NK.Hash spezifiziert die Hashalgorithmen, die im Rahmen der Integritätssicherung zum Einsatz kommen. Hier ist anzumerken, dass der Schutz der Integrität im Rahmen von IPsec durch das Protokoll IP Encapsulating Security Payload (ESP) (RFC 4303 (ESP), [51]) 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 die verschlüsselten Nutzdaten des Paketes ergibt. Insofern ist eine Hashfunktion erforderlich. Weiterhin ist im IPSec sowie in IKE Standard die Verwendung von HMAC Algorithmen enthalten ([55], [56], [52]). 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
	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*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	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*	

EVG-Ziel	Aspekt des Ziels	SFR, SAR (vgl. Abschnitt 6.2 oder 6.4)
	maintain a set of packet filtering rules …“). Der dynamische Aspekt wird durch FDP_IFF.1.4/NK.PF (*Stateful Packet Inspection*) abgebildet und durch das folgende Refinement präzisiert. Der Paketfilter ist als Sicherheitsfunktion nur dann wirksam, wenn er auf Basis geeigneter Filterregeln arbeitet. Dem tragen die folgenden Komponenten FMT_MSA.3/NK.PF und FMT_MSA.1/NK.PF Rechnung: FMT_MSA.3/NK.PF trägt als von FDP_IFF.1/NK.PF abhängige Komponente zur Sicherheit bei, indem sie restriktive Voreinstellungen für die Filterregeln fordert. FMT_MSA.1/NK.PF beschränkt die Möglichkeiten zur Administration der Filterregeln auf gewisse Rollen. FMT_SMR.1./NK wiederum listet alle Rollen auf, die der EVG kennt, und fordert so die Modellierung der Rollen durch EVG. FMT_SMF.1/NK (als von FMT_MSA.1/NK.PF abhängige Komponente) listet alle administrativen Funktionen auf. *„Für zu schützende Daten der TI und der Bestandsnetze sowie zu schützende Nutzerdaten bei Internet-Zugriff über den SIS erzwingt der EVG die Nutzung eines VPN-Tunnels. Ungeschützter Zugriff von IT-Systemen aus dem LAN (z. B. von Clientsystemen) auf das Transportnetz wird durch den EVG unterbunden: IT-Systeme im LAN können nur unter der Kontrolle des EVG und im Einklang mit der Sicherheitspolitik des EVG zugreifen.*“ → Dies wurde teilweise durch FDP_IFF.1.3/NK.PF modelliert (zwangsweise Nutzung des VPN-Tunnels). Ferner ist die Sicherheitsleistung des Paketfilters natürlich abhängig von den verwendeten Paketfilterregeln. Daher beschränkt der EVG die Administration gewisser grundlegender Paketfilterregeln; siehe dazu das Refinement zu FMT_MSA.1/NK.PF. Für die Paketfilterregeln, die der Administrator administrieren darf, informiert ihn die Benutzerdokumentation hinreichend; siehe dazu das Refinement zu AGD_OPE.1 (Administration der Paketfilter-Regeln) in Abschnitt 6.4.2.	

Tabelle 28: Abbildung der EVG-Ziele auf Anforderungen

Anwendungshinweis 205: Hinweis zu O.NK.VPN_Integrität: Wird zur Erfüllung der Anforderungen aus FCS_COP.1/NK.Hash eine Hashfunktion verwendet, die nicht auf einem symmetrischen Verschlüsselungsalgorithmus beruht, sind keine geheimzuhaltenden Schlüssel erforderlich. Wird eine Hashfunktion verwendet, die auf einem symmetrischen Verschlüsselungsalgorithmus beruht, ergeben sich die üblichen Abhängigkeiten (FCS_CKM.1/NK, FCS_CKM.4/NK); in diesem Fall soll der ST-Autor diese Abhängigkeiten in Tabelle 26 aufnehmen und in Tabelle 28 (oben) begründen.

6.5.6. 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 [68] bzw. [74] 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 [68].
- FCS_CKM.1/NK.TLS fordert die kryptographische Schlüsselgenerierung von 128 und 256 Bit Schlüsseln gemäß [74].
- 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.PKCS.SigPr fordert die Verwendung der Verfahren PKCS#1 und SHA-2 für die Prüfung von digitalen Signaturen über gegebene Daten.
- 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 [68] 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 [68] 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 [68] 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 [68] 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 [68] 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 Signaturrichtlinein sind durch FMT_SMF.1/**AK** gefordert.
- Die Rolle des Administrators ist durch FMT_SMR.1/**AK** und die Managementfunktionen des EVG, insbesondere das Management der eHealth-Kartenterminals und der Arbeitsplätze, sind durch FMT_SMF.1/**AK** gefordert.

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 [67]. Die Forderungen aus [67] werden insbesondere durch folgende SFR umgesetzt.

- FIA_API.1/AK fordert, dass die TSF sich gegenüber der QSEE für die Stapelsignatur authentisiert.
- FIA_UAU.5/**AK** beschreibt die Forderung der Authentisierung des HBA vor Ausführung einer Stapelsignatur, und außerdem den Schutz von Vertraulichkeit und Integrität der Kommunikation (insbesondere mit der QSEE) zu schützen.
- FDP_ACF.1/AK**.Sgen** und FMT_MSA.4/**AK** fordern von der TSF zu überprüfen, ob für die Daten des Stapels ordnungsgemäße qualifizierte elektronische Signaturen erstellt wurden. Bei festgestellten Abweichungen sind alle durch die aktuelle Signtaur-PIN-Eingabe autorisierte Signaturen zu verwerfen. FDP_ACC.1/AK**.Sgen** identifiziert die Signaturerstellungs-SFP.
- FDP_ACF.1/AK**.Sgen** fordert von der TSF, den Sicherheitszustand der QSEE, der nach erfolgreicher Authentisierung des Signaturschlüssel-Inhabers erlangt wurde, nach der Abarbeitung des Stapels zurückzusetzen.
- Das Clientsystem ist über festgestellte Abweichungen beim Signaturprozess über die Schnittstelle gemäß FTA_TAB.1/AK**.SP** zu informieren.
- FTP_ITC.1/AK**.**QSEE fordert die Einrichtung eines vertrauenwürdigen Kanals zwischen EVG und QSEE zum Schutz der zu signierenden Daten.

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 [68] 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 nichtqualifizierter elektronischer Signaturen für die Benutzer gemäß gültiger Signaturrichtlinien bereitzustellen.
- Für die Prüfung der digitalen Signaturen der signierten Daten muss die TSF die kryptographischen Operationen gemäß FCS_COP.1/AK.SHA, FCS_COP.1/AK.SigVer.PSS, FCS_COP.1/AK.SigVer.ECDSA und FCS_COP.1/AK.SigVer.SSA implementieren.
- Für die Prüfung der XML-kodierten signierten Daten muss die TSF FCS_COP.1/AK.XML.SigPr implementieren. Für CMS bzw. PKCS#1 kodierte signierte Dokumente ist dies entsprechend in FCS_COP.1/AK.CMS.SigPr bzw. FCS_COP.1/AK.PKCS.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 [32] und [68].
- 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 [69] 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/AK**.Update** führt die Update-SFP für den Software-Update ein und

FDP_ACF.1/AK**.Update** definiert die Regeln für den Umgang mit dem Software-Update beim Import. Die Anforderung FDP_UIT.1/AK**.Update** fordert den Empfang der Software-Update-Daten und die Prüfung der Integrität dieser Daten vor dem Update. Die Anforderungen FTP_ITC.1/AK.KSR und FTP_TRP.1/NK.Admin fordern einen gesicherten Kanal für den Empfang der Software-Update-Daten aus der TI bzw. lokal über die Management-Schnittstelle. FPT_TDC.1/**AK** fordert die Fähigkeit des EVG zur Interpretation, und damit dem Import und die Aktualisierung von TSL und CRL nach erfolgreicher Prüfung der entsprechenden Signaturen und Zertifikate. FTP_ITC.1/AK.KSR und FTP_ITC.1/AK.TSL fordern den Aufbau eines sicheren Kanals für den Download von Firmware-Update-Paketen bzw. der BNetzA-VL und deren Hash-Wert.

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**.

6.5.7. Erklärung für die Vertrauenswürdigkeitsanforderungen

Der Schutz der Benutzerdaten durch Verschlüsselung erfordert einen Schutz gegen ein Angriffspotential „Enhanced Basic“. Für CC Version 3.1 ist folglich eine Erweiterung der gewählten EAL-Stufe EAL3 um AVA_VAN.3 notwendig. Daraus ergeben sich Abhängigkeiten gem. [3], die mit den zusätzlichen Erweiterung um ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 und ALC_TAT.1 aufgelöst werden.

Anmerkung: Die in CC Teil 3 [3] angegebenen Abhängigkeiten von AVA_VAN.3 sind leider nicht vollständig aufgelöst: ADV_IMP.1 impliziert zusätzlich ALC_TAT.1.

Die Komponente ALC_FLR.2 wurde gewählt, um Prozeduren zur Beseitigung von festgestellten Sicherheitsproblemen und Verbesserungen des EVG auf der Grundlage von Informationen der Anwender reagieren zu können und zur Verbesserung des EVG beizutragen. ALC_FLR.2 besitzt keine weiteren Abhängigkeiten.

Die EAL-Stufe an sich ist in sich konsistent und erfüllt alle Abhängigkeiten.

Die hier beschriebenen Vertrauenswürdigkeitskomponenten entsprechen den gewählten Vertrauenswürdigkeitskomponenten in Kapitel 6.4.

7. Anhang

7.1. Auszüge aus der Konnektorspezifikation [76] zum Zugriffsberechtigungsdienst

Die Inhalte, die in diesem Abschnitt dargestellt werden, sind der Spezifikation Konnektor [gemSpec_Kon] [76], 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

Entität	persistent/ transient	Identitäts -schlüssel	Beschreibung
			gleichzeitig, genutzt werden, z. B. bei 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 29: TAB_KON_507 Informationsmodell Entitäten aus [76]

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.

Attribut	Beschreibung
mandantId	Das Identifikationsmerkmal eines Mandanten. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.
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 30: TAB_KON_508 Informationsmodell Attribute aus [76]

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 31: TAB_KON_509 Informationsmodell Entitätenbeziehungen aus [76]

#	Beschreibung	Definition mittels OCL[464]
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)
C11	Die Identifikationsnummer (slotNo) des Kartenterminal-Slots für ein gegebenes Kartenterminal muss eindeutig sein.	**context** Kartenterminal **inv:** self.kT-Slot ->\ isUnique(slotNo)

[464] Die Constraints werden im UML ergänzenden Standard OCL definiert.

#	Beschreibung	Definition mittels OCL[464]
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 32: TAB_KON_510 Informationsmodell Constraints aus [76]

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: 3. Ermittle Zugriffsregel R zu den Aufrufparametern: 3.1. 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 33: TAB_KON_511 - TUC_KON_000 „Prüfe Zugriffsberechtigung“ aus [76]

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 34: 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 35: TAB_KON_513 Zugriffsregeln Regelzuordnung aus [76]

	Bedingung[465]	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
Entität[466]	`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`
	`= Kartenterminal(ctId)`
	`inv : kt <> null`
			x		x						4007

	`let k : Karte = Karte(cardHandle)` `inv : k <> null`					x	x	x	x	x	4008

465 Jede Bedingung ist als Constraint mittels OCL definiert, ist einzeln prüfbar und hat als Eingangsparameter mandantId, clientSystemId, workplaceId, ctId, cardHandle und userId.

466 Zur Bezeichnung einer Objektinstanz, die im Informationsmodell vorhanden ist, wird die Notation <<Entitätsbezeichner>>(<<Komma separierte Liste der Identitätsschlüssel>> verwendet.

	Bedingung[465]	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
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
	let m : Mandant = Mandant(mandantId) let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) inv : ap.mandant.includes(m)			x	x	x	x	x	x	x	4011
	let m : Mandant = Mandant(mandantId) let kt : Kartenterminal = Kartenterminal(ctId) inv : kt.mandant.includes(m)		x		x						4012
	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
	let m : Mandant = Mandant(mandantId) let k : Karte = Karte(cardHandle) inv : k.SM-B_Verwaltet.mandant -> includes(m)							x			4013
	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
	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let kt : Kartenterminal = Kartenterminal(ctId) inv : ap.lokalKartenterminal.includes(kt) or ap.entferntKartenterminal.includes(kt)				x						4015
	let ap : Arbeitsplatz = Arbeitsplatz(workplaceId) let kt : Kartenterminal = Karte(cardHandle).kT-Slot.kartenterminal inv : ap.lokalKartenterminal.includes(kt) or ap.entferntKartenterminal.includes(kt)							x	x	x	4015
	let m : Mandant = Mandant(mandantId) let kt : Kartenterminal = Kartenterminal(ctId)		x								4020

	Bedingung[465]	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
	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)										
	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 36: TAB_KON_514 Zugriffsregeln Definition aus [76]

7.2. 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
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

Abkürzung	Bedeutung
	im Kontext digitaler Signaturen: Cryptographic Message Syntax
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)
gematik	gematik GmbH, siehe https://www.gematik.de/
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
RAD	reference authorisation data (Authentisierungsreferenzdaten)

Abkürzung	Bedeutung
SE	Security environment
SAK	Bezeichnung einer Identität des Konnektors; steht für Signaturanwendungskomponente, 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 **a**nd 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 (Authentisierungs-verifikationsdaten 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

Abkürzung	Bedeutung
VSDM	Versichertenstammdatenmanagement, siehe auch Fachmodul
VSDD	Versichertenstammdatendienst, siehe auch Fachdienst
XAdES	XML Advanced Electronic Signature: ETSI Standard zur Signatur von XML Dokumenten
XAdES-X	XAdES extended: ein Profil von XAdES
xTV	Veraltete Bezeichnung eines Teils einer SAK gemäß SigG/SigV. Extended Trusted Viewer (erweiterte sichere Anzeige) als Teil des Konnektors, ausgelagert auf den Arbeitsplatz des Benutzers. Diese Funktionalität kann nun von einer Clientsoftware umgesetzt werden und gehört nicht zum EVG.

7.3. Glossar

Begriff	Definition
Ablauflogik	Der Begriff Ablauflogik bezeichnet die Möglichkeit, erlaubte Reihenfolgen von Basisdiensten und Fachdiensten vorzugeben. Welche Abläufe dies im Einzelnen sind, hängt von den konkreten fachlichen Anwendungsfällen ab. Die Ablauflogik kann außerhalb der TSF liegen, die Ablaufkontrolle ist Teil der TSF. Häufig wird der Begriff Ablauflogik auch synonym zum Begriff Fachlogik verwendet.
Anwendungs-konnektor	Der Teil des Konnektors [76], der dem Clientsystem die Schnittstellen zu den Fachdienstmodulen (VSDD, AMTS etc.) und Basisdienste (Sicherheitsdienste, Chipkartendienste, Kartenterminaldienste, Hilfsdienste) zur Verfügung stellt und die dafür notwendigen Managementdienste implementiert.
Authentisierungs-referenzdaten	Daten, die zur Prüfung der Authentisierungsdaten benutzt werden. Die Integrität dieser Authentisierungsreferenzdaten ist zu schützen. Englisch: authentication reference data, abgekürzt RAD.
Authentisierungs-verifikationsdaten	Daten, die vom Benutzer zum Nachweis seiner Identität gegenüber dem Kartenterminal präsentiert werden, z.B. eine PIN oder biometrische Merkmalsdaten. Englisch: authentication verification data, abgekürzt SVAD.
Autorisierter Benutzer des Clientsystems	Ein Benutzer des Clientsystems ist dann für die Auslösung des Signaturprozesses autorisiert, wenn der Benutzer durch den EVG identifiziert wurde, sich für den Vorgang, der durch die am eHealth-Kartenterminal angezeigte Jobnummer identifiziert wurde, gegenüber dem zugeordneten Heilberufsausweis erfolgreich mit der PIN.QES authentisiert hat (vergl. [67]).
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 Signatur-dienst an die Signaturkarte zum Signieren gesendet wird.

Begriff	Definition
	Umfasst der Stapel zu signierender Daten mehr Daten als durch die Zugriffsbedingung der Signaturkarte nach eine Authentisierung mit der Signatur-PIN zulässig sind, ist die Authentisierung mit der Signtaur-PIN zu wiederholen oder Prozess der Signaturerstellung abzubrechen (s.a. Anwendungshinweis 191).
Bestandsnetz	Bereits vor Einführung der Telematikinfrastruktur bestehende Netze deren Anwednungen durch Leistungserbringer genutzt werden und über die Telematikinfrastruktur zugänglich sind.
Kartenhandle (BKH)	Handle zur Identifizierung einer Chipkarte, die in einem eHealth-Kartenterminal steckt. Mit diesem BKH sind folgende Informationen verknüpft (s. [76], 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. [76], Kap. 4.1.5.4.7): (1) einseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, (2) einseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, (3) gegenseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, (4) gegenseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, (5) gegenseitige asymmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals, (6) gegenseitige symmetrische Authentisierung mit Aushandlung eines Sessionkey (Trusted Channel Schlüssel der Quellchipkarte und Secure Messaging Schlüssel der Zielchipkarte) und Aufbau eines Secure Messaging Kanals. Die externe Authentisierung mit Ausnahme von (5) verändert den Authentisierungsstatus der prüfenden Chipkarte.
Chipkarte	In diesem Schutzprofil: der Heilberufsausweis (HBA), SMC-Typ B, eGK und KVK.
CRL Download Server	Ein von der PKI der TI bereitgestellter Downloadpunkt im Internet, von dem der Konnektor die aktuelle CRL erhalten kann.
Digitale Signaturen	Asymmetrischer kryptographischer Mechanismus bei dem für Daten („Nachricht“) ein Datum („Signatur“) mit Hilfe eines geheimen Signaturschlüssels („Signaturerstellungsdaten“) berechnet und der Nachricht zugeordnet werden, und diese Zuordnung bei Kenntnis der Nachricht und der Signatur mit dem zum Signaturschlüssel zugehörigen öffentlichen Signaturprüfschlüssel geprüft werden kann.

Begriff	Definition
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 [77], evaluiert gemäß [71] 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 eine Chipkarte (PIN-Empfänger) in einem anderen Chipkarten-Terminal unter Steuerung der AK (s. [67], Kap. 2.1.2, und [76], 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 (Verordnungsdaten-management, VODM), • Berechtigungsnachweis zur Inanspruchnahme von Leistungen (Versichertenstammdatenmanagement, VSDM), • Notfallversorgung (Notfalldatenmanagement, NFDM), • Arztbrief • Arzneimitteltherapiesicherheit • elektronische Patientenakte • Versichertendaten • in Anspruch genommene Leistungen und deren vorläufige

Begriff	Definition
	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*: Gültige Zertifikate müssen im Zertifikatsverzeichnis des ausstellenden qualifizierter Vertrauens-diensteanbieters 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.

Begriff	Definition
	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 [80] und [82], dessen Betriebssystem nach PP COS G2 [70] 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. [76], 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 [76].
Krankenversicherten-karte (KVK)	Chipkarte mit eingeschränkter Funktionalität, die die Identität des Versicherten speichert. Die KVK besitzt kein EF.ATR, EF.GDO und EF.DIR und kann keine PIN-Authentisierung, Card-to-Card-Authentisierung und keine Zugriffskontrolle durchführen.
Leistungserbringer	Verantwortlicher für die Einsatzumgebung der dezentralen Komponenten Konnektor, eHealth-Kartenterminal und SMC Typ B

Begriff	Definition
	sowie der Clientsysteme und des lokalen Netzes.
lokale PIN-Eingabe	Die PIN-Eingabe erfolgt an dem Chipkartenterminal, in welchem sich die Chipkarte befindet, die die PIN prüfen soll. Die lokale PIN-Eingabe nutzt den sicheren Eingabe-Modus der eHealth-Kartenterminals und darf die PIN sowohl unverschlüsselt als auch mit den Prozeduren der entfernten PIN-Eingabe verschlüsselt an den PIN-Empfänger übergeben.
Managementschnitt-stelle	(herstellerspezifische) äußere logische Schnittstelle für alle Managementfunktionen einschließlich Administratorfunktionen.
Ordnungsgemäße qualifizierte elektronische Signaturen eines Signaturstapel	Ordnungsgemäße qualifizierte elektronische Signaturen sind solche fortgeschrittene elektronische Signaturen, die zu den Daten des Signaturstapels mit dem Signaturschlüssel des Heilberufsausweises des autorisierten Benutzers des Clientsystems erzeugt wurden und zu dessen Signaturprüfschlüssel zum für die Signatur festgelegten Zeitpunkt ein gültiges qualifiziertes Zertifikat existiert.
PIN-Empfänger	Chipkarte, die eine verschlüsselte PIN oder PUK verschlüsselt für die PIN-Prüfung oder den PIN-Wechsel oder das Entblockieren einer PIN empfängt. Ein PIN-Empfänger ist ein HBA oder eine SMC-B (oder ein RFID-Token für die Komfortsignatur, wenn der EVG Komfortsignatur mit derartigen Token unterstützt).
PIN-Sender	Chipkarte, die eine PIN oder PUK unverschlüsselt empfängt und verschlüsselt für die Übertragung an den PIN-Empfänger ausgibt. Ein PIN-Sender ist eine gSMC-KT.
Clientsystem	Komponente mit einem Benutzerinterface für fachliche Funktionalität. Die Clientsysteme der Leistungserbringer umfassen die Praxisverwaltungssysteme, für Ärzte und Zahnärzte, die Krankenhausinformationssysteme der Krankenhäuser und die Apothekenverwaltungssysteme der Apotheker und stellen die Anwendungsprogramme für die Leistungserbringer und Versicherten zur Verfügung. Sie sind über das LAN des Leistungserbringers mit dem Konnektor verbunden.
qualifizierte elektronische Signaturen	Fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht, vgl. eIDAS [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 Vertrauensdienste-	„Qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte

Begriff	Definition
anbieter	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. [82], Kap. 9).
qualifizierte elektronische Signaturerstellungs-einheit	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 [77], in dem das eHealth-Kartenterminal durch ein SICCT-Kommando [79] angewiesen wird, die Tastatureingabedaten in einem angegebenen Chipkartenkommando an eine Chipkarte in einem angegebenen Chipkartensteckplatz zu senden und die Antwort der Chipkarte zurückzugeben. Der sichere PIN-Modus ist dem Benutzer anzuzeigen und muss die Vertraulichkeit der Tastatureingabedaten schützen.
Signaturanwendungs-komponenten	Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate Englisch: SCA und SVA, hier als SCaVA abgekürzt.
Signaturattribute	Dieser Begriff wird hier verwendet, um die Arten der Signaturen „einfache Dokumentensignatur“, „Parallelsignatur“ und „Gegensignatur“ zu unterscheiden. Sicherheitsattribute sind Bestandteil der Signaturrichtlinie.
Signaturchipkarte	Chipkarte mit privaten Schlüsseln zur Erstellung digitaler Signaturen einer elektronischen Signatur. Dies sind gegenwärtig der HBA mit dem privaten Schlüssel PrK.HP.QES, die SMC Typ B mit dem privaten Schlüssel PrK.HI.OSIG und die eGK mit dem privaten Schlüssel PrK.CH.QES.
Signaturrichtlinie	Die Signaturrichtlinie (Profilierung der Signaturformate) identifiziert - den Typ der Signatur als nicht-qualifizierte oder qualifizierte elektronische Signatur, und kann weitere Informationen umfassen (s. [76], Anhang B) wie z.B. - Anforderungen an Zertifikatsreferenzen

Begriff	Definition
	- 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 [80] und [83], dessen Betriebssystem nach PP COS G2 [70] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.
SMC Typ KT (gSMC-KT)	Sicherheitsmodul des Kartenterminals. Chipkarte gemäß Spezifikation [80] und [85], dessen Betriebssystem nach PP COS G2 [70] 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“

Begriff	Definition
	gegenüber dem HBA benötigt werden. Chipkarte gemäß Spezifikation [80] und [84], dessen Betriebssystem nach PP COS G2 [70] und dessen Objektssystem nach BSI TR-03144 zertifiziert wurden.
Stapel zu signierender Daten	Liste zu signierender Daten, die durch den Benutzer des Clientsystems ausgewählt wurden und über das Clientsystem an den EVG gesendet wurden.
Stapelsignatur	Erstellung einer begrenzten Anzahl Signaturen nach den zeitlich unmittelbar aufeinander folgenden Prozessen der Übergabe der zu signierenden Daten an den EVG über das Clientsystem und der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der QSEE.
stateful packet inspection, stateful inspection	dynamische Paketfiltertechnik, bei der (sofern es die Systemressourcen zulassen; im Fall eines denial-of-service-Angriffs müssen Datenpakete verworfen werden) jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird; der Verbindungsstatus eines Datenpakets wird in die Entscheidung einbezogen, ob ein Informationsfluss zulässig ist oder nicht
Statusmeldungen	Durch den EVG generierte Meldungen an Benutzer zu Fehlern bei der Erfüllung angeforderter Sicherheitsdienst (z. B. nicht gefundene oder ungültige Zertifikate vorgesehener Empfänger zu verschlüsselnder Daten).
Telematikinfrastruktur (TI)	Die Telematikinfrastruktur ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen und organisatorischen Anteilen. Die Telematikinfrastruktur vernetzt alle Akteure und Institutionen des Gesundheitswesens miteinander und ermöglicht dadurch einen organisationsübergreifenden Datenaustausch innerhalb des Gesundheitswesens.
TI Services	zentrale Dienste und Fachdienste der Telematikinfrastruktur
Trust-Service Status List (TSL)	Die Trust-service Status List enthält die öffentlichen Schlüssel aller vertrauenswürdigen CAs, die Information über den für diese CA akkreditierten Zertifikatstyp sowie die Adresse der Zertifikats Status Services (OCSP-Responder und CRL Provider). Sie ist durch gematik TSL Serviceprovider signiert.
Trusted Service Provider (TSP)	TSPs sind Stellen, die innerhalb oder im Auftrag der Teilnehmerorganisationen Zertifikate für natürliche oder juristische Personen oder technische Komponenten ausstellen und/oder Verzeichnisdienste betreiben.
Update-Daten	Update-Daten bestehen aus Updateinformation und Updatepaket, die gesondert integritätsgeschützt sind.
Verschlüsselungs-richtlinie	Verschlüsselungsrichtlinie, die beschreiben • das Verschlüsselungsformat (EncryptionType): Cryptographic Message Syntax [33], XML-Encryption [21] oder S/MIME [34],

Begriff	Definition
	• für XML-Encryption: - XML-Schema: beschreibt die zu verschlüsselnden bzw. zu entschlüsselnden Daten, - Option: KeyInfo im XML-Dokument oder nicht • Herausgeber der Verschlüsselungsrichtlinie.
Vertrauensanker	Öffentlicher Schlüssel oder Zertifikat (in dem sich ein öffentlicher Schlüssel befindet), das als letzte Instanz bei der Prüfung einer Zertifikatskette in einer PKI zum Einsatz kommt. Dies kann bspw. der öffentliche Schlüssel eines Wurzel-Zertifikats (Root-CA) oder ein Signer-Zertifikat einer Liste von CAs (bspw. BNetzA-VL oder TSL) sein.
Vertrauensliste der Bundesnetzagentur (BNetzA-VL)	Vertrauensliste der Bundesnetzagentur mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die von der Bundesrepublik Deutschland beaufsichtigt werden, sowie mit Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten, vgl. eIDAS Artikel 22.
Vertrauensdienste-anbieter	„Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt, vgl. eIDAS [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 Verschlüs-selungsrichtlinie	Eine Verschlüsselungsrichtlinie ist zulässig, wenn die Regeln auf die zu verschlüsselnden oder zu entschlüsselnde Daten anwendbar sind. Die Installation der Verschlüsselungsrichtlinie erfolgt mit der Installation oder Update des EVG oder der Fachanwendung, die diese Verschlüsselungsrichtlinie implementiert.

7.4. Abbildungsverzeichnis

7.5. Tabellenverzeichnis

7.6. Literaturverzeichnis

7.6.1. 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

7.6.2. 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 https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf

[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)

7.6.3. 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 SP 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 8446 (August 2018): The Transport Layer Security (TLS) Protocol, Version 1.3

[33] RFC 5652 (September 2009): Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc5652.txt

[34] 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)

[35] 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

[36] 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

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

[38] SEC 1: Elliptic Curve Cryptography, Certicom Research. Version 2.0, 21.05.2009, http://www.secg.org/download/aid-780/sec1-v2.pdf

[39] 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

[40] TIFF Revision 6.0, http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

[41] Unicode Standard Version 6.2.0. http://www.unicode.org/versions/Unicode6.2.0/

[42] 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

[43] 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

[44] 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

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

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

[47] 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

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

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

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

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

[52] 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

[53] 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

[54] 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

[55] 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

[56] 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

[57] 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

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

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

[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] R. Housley: Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, RFC 5083, November 2007, https://tools.ietf.org/html/rfc5083

[64] 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

7.6.4. Schutzprofile (Protection Profiles) und Technische Richtlinien

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

[66] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.0, 28.08.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[67] BSI TR-03114 Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[68] 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)

[69] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, BSI-CC-PP-0097, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.6.4, 17.03.2020

[70] Common Criteria Schutzprofil (Protection Profile) Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V3-2018, Version 2.0, 10.07.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[71] Protection Profile Electronic Health Card Terminal, BSI-PP-0032, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.7, 21.09.2016

[72] 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

7.6.5. Spezifikationen

[73] Einführung der Gesundheitskarte: Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP], Version 2.10.0, 02.03.2020, gematik GmbH

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

[75] Einführung der Gesundheitskarte: Produkttypsteckbrief Konnektor [gemProdT_Kon_PTV3.6.0-2], Version 1.0.0, 04.03.2020, gematik GmbH

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

[77] Einführung der Gesundheitskarte. Spezifikation eHealth-Kartenterminal [gemSpec_KT], Version: 3.12.0, Stand: 02.03.2020, gematik GmbH

[78] Einführung der Gesundheitskarte: Spezifikation Fachmodul VSDM [gemSpec_FM_VSDM], Version 2.5.0, 15.05.2019, gematik GmbH

[79] 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

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

[81] Einführung der Gesundheitskarte: Spezifikation der elektronischen Gesundheitskarte – eGK-Objektsystem [gemSpec_eGK_ObjSys], Version 3.12.0, 15.05.2019, gematik GmbH

[82] Einführung der Gesundheitskarte: Spezifikation des elektronischen Heilberufsausweises – HBA-Objektsystem [gemSpec_HBA_ObjSys], Version 3.13.0, 15.05.2019, gematik GmbH

[83] Einführung der Gesundheitskarte. Spezifikation der Security Module Card SMC-B Objektsystem [gemSpec_SMCB_ObjSys], Version 3.13.0, 15.05.2019, gematik GmbH

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

[85] Einführung der Gesundheitskarte. Spezifikation der gSMC-KT – Objektsystem [gemSpec_gSMC-KT_ObjSys], Version 3.9.0, 24.08.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[86] Einführung der Gesundheitskarte. Übergreifende Spezifikation: Operations und Maintenance [gemSpec_OM]. Version 1.13.0, Stand 02.03.2020, gematik GmbH

[87] Einführung der Gesundheitskarte. Spezifikation TSL-Dienst [gemSpec_TSL]. Version 1.17.0, Stand 02.03.2020, gematik GmbH

[88] Einführung der Gesundheitskarte. Spezifikation Verzeichnisdienst [gemSpec_VZD]. Version 1.9.0, Stand 02.10.2019, gematik GmbH

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