Common Criteria Certification
BSI-DSZ-CC-1068 BSI-CC-PP-0098

Security Target
Konnektor

KoCoBox MED+ OPB 2.1 KONNEKTOR
Version 2.3.24

KoCo Connector GmbH
Dessauer Str. 28/29
10963 Berlin
info@kococonnector.com

Dokumentversion 1.27
2020-07-16

Vorwort

Anmerkungen zur CC Zertifizierung

Die vorliegende *KoCoBox MED+* wird in zwei Verfahren zertifiziert: Das umfassende Verfahren nach [BSI-CC-PP-0098] beschreibt die gesamte Firmware des Konnektors. Dieses Schutzprofil fordert eine Evaluierung nach AVA_VAN.3. Zusätzlich dazu gibt es ein zweites, spezialisiertes Verfahren, in dem die Anforderungen an die Komponente „Netzkonnektor“ spezifiziert werden. Dieses Verfahren wird nach den Vorgaben des Schutzprofils [BSI-CC-PP-0097] durchgeführt, das eine Evaluierung nach AVA_VAN.5 vorsieht.

Das Schutzprofil [BSI-CC-PP-0097] stellt eine Teilmenge des Schutzprofils [BSI-CC-PP-0098] dar. Abbildung 0.1 zeigt schematisch, welche Teile des Konnektors von welchem Schutzprofil beschrieben werden und wie sich die Schutzprofile zueinander verhalten.

Zur Vereinfachung der beiden Verfahren folgen die Security Targets der Struktur der Schutzprofile: Das Security Target für den Gesamtkonnektor [KoCo ASE_ST-98] enthält auch den gesamten Inhalt des Security Targets für den Netzkonnektor [KoCo ASE_ST-97]. Bis auf minimale orthographisch bedingte Abweichungen sind die Texte strukturell identisch. Lediglich an den Stellen, an denen auf den jeweiligen TOE Bezug genommen wird, weichen die Texte voneinander ab.

*Das Security Target des **Netzkonnektors** bezieht sich bei allen Bedrohungen, Annahmen, Sicherheitszielen und Anforderungen auf (a) das Schutzprofil des Netzkonnektors und (b) auf genau die Teile des Schutzprofiles des Gesamtkonnektors, die sich auf den Netzkonnektor beziehen. Dieser doppelte Bezug wird angenommen, ohne eine formale Übereinstimmung zu behaupten.*

*Das Security Target des **Gesamtkonnektors** hingegen bezieht sich an allen Stellen, die auch in [KoCo ASE_ST-97] beschrieben sind, ebenfalls auf beide Schutzprofile.*

Ziel dieser Maßnahme ist, dass ein Evaluator lediglich die Dokumente für den Gesamtkonnektor [KoCo ASE_ST-98] zugrunde legen muss, um den vorliegenden Evaluierungsgegenstand nach *beiden* Schutzprofilen, bzw. Security Targets bewerten zu können.

Diese Einführung mit der Abgrenzung gegenüber den Schutzprofilen ersetzt nicht die formale Behauptung der Konformität zu einem Schutzprofil. Diese geht aus den Ausführungen in Kapitel 2 hervor.

Anmerkungen zur TR Zertifizierung

Die KoCoBox MED+ dient als Ablaufplattform für die Fachmodule NFDM und AMTS [gemSpec_FM_NFDM; gemSpec_FM_AMTS]. Diese Fachmodule sind nicht Teil der Common Criteria Zertifizierung des Gesamtkonnektors. Stattdessen werden sie nach den Technischen Richtlinien *Konnektor – Prüfspezifikation für das Fachmodul NFDM* und *Konnektor – Prüfspezifikation für das Fachmodul AMTS* zertifiziert [TR-03154; TR-03155]. Die TR stellen Anforderungen an die CC-Zertifizierung des Konnektors: Der Konnektor muss bestimmte Eigenschaften aufweisen. Es ist Aufgabe des CC-Zertifzierers, die Erfüllung dieser Anforderungen zu bestätigen.

Obwohl keine formale Übereinstimmung mit den TR behauptet wird, spielen die TR eine wichtige Rolle für die CC-Zertifzierung. Das drückt sich in diesem Security Target dadurch aus, dass die Konformitätserklärung in Kapitel 2 um einen Abschnitt erweitert wurde. Weiterhin wird in Kapitel 8 beschrieben, wie die KoCoBox MED+ die Anforderungen erfüllt.

Anmerkungen zur Spezifikationslage

Die KoCoBox MED+ wurde nach der Spezifikation der gematik entwickelt. Dabei gelten die Spezifikationsdokumente in Tabelle 0.1.

Dokument	Version	Datum	Referenz
Produkttypsteckbrief Konnektor, Produkttyp Version PTV3 3.6.0-2	1.0.0	4. März 2020	[gemProdT_Kon_PTV3_3.6.0-2]
Spezifikation Konnektor	5.4.0	26. Okt. 2018	[gemSpec_Kon]
Errata 1 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.1	6. Feb. 2019	[gemErrata_1_Kon_PTV3]
Errata 2 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.0	6. Juni 2019	[gemErrata_2_Kon_PTV3]
Errata 3 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.0	2. Okt. 2019	[gemErrata_3_Kon_PTV3]
Errata 4 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.1	27. Nov. 2019	[gemErrata_4_Kon_PTV3]
Errata 5 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.0	4. Feb. 2020	[gemErrata_5_Kon_PTV3]
Errata 6 zum Konnektor PTV 3 (eMP/AMTS, NFDM)	1.0.0	4. März 2020	[gemErrata_6_Kon_PTV3]

Tabelle 0.1.: Spezifikationsdokumente der KoCoBox MED+

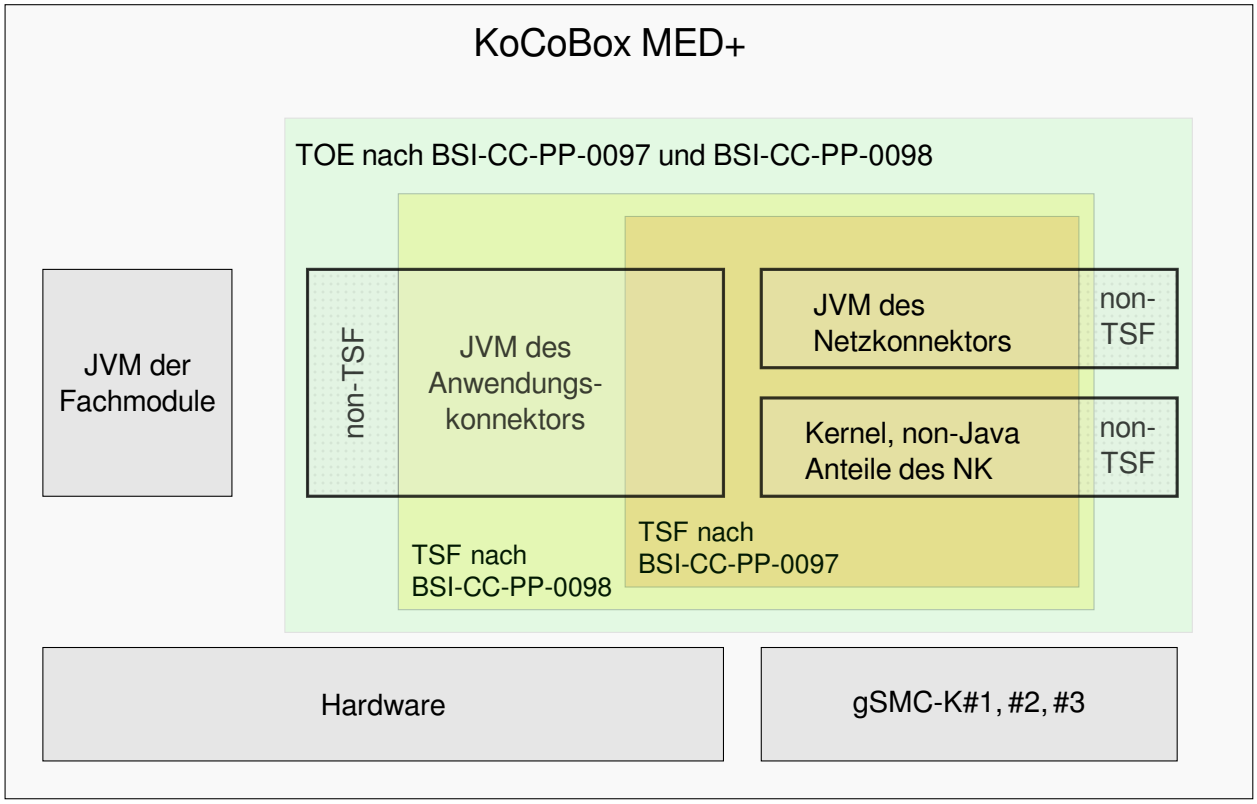


Abbildung 0.1.: Abgrenzung der Verfahren zu BSI-CC-PP-0097 und BSI-CC-PP-0098

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einführung in das Security Target

Der TOE, der in diesem Dokument beschrieben wird, ist der *KoCoBox MED+ OPB 2.1 Konnektor*. Der TOE ist eine sichere Komponente, die im Kontext der Telematikinfrastruktur als Konnektor eingesetzt wird.

Dieses Dokument ist das *Security Target*, in dem die funktionalen und organisatorischen Sicherheitsanforderungen des TOE und seiner Einsatzumgebung beschrieben werden. Dieses Dokument findet seine formale Grundlage in:

- *Schutzprofil 2: Anforderungen an den Konnektor* [BSI-CC-PP-0098]

Darüber hinaus gibt es – wie im Vorwort beschrieben – eine enge Verwandtschaft zum Dokument *Schutzprofil 1: Anforderungen an den Netzkonnektor* [BSI-CC-PP-0097].

1.1. ST Referenz

Titel des Dokuments	Security Target / Konnektor
Version des Dokuments	1.27
Datum des Dokuments	16.07.2020
Allgemeiner Status:	Verfeinerung nach der Einreichung für den Antrag des Zertifizierungsverfahrens
Autor	KoCo Connector GmbH
Editor	n-design GmbH, OS-Cillation GmbH

1.2. TOE Referenz

Evaluierungsgegenstand	KoCoBox MED+ OPB 2.1 Konnektor
Version des EVG	2.3.24
Hersteller	KoCo Connector GmbH
Vertrauenswürdigkeitsstufe	EAL3 erweitert um AVA_VAN.3, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 (Kurzbezeichnung „EAL3+“)
CC Version	3.1 Release 5

1.3. Überblick über den TOE

Der Evaluierungsgegenstand ist der Konnektor für den Online Produktivbetrieb Stufe 2.1. Der TOE umfasst folgende Komponenten:

- den Netzkonnektor
- den Anwendungskonnektor
- das Fachmodul „Versichertenstammdatenmanagement“ (VSDM)

Der Lieferumfang des TOE umfasst ebenfalls die Betriebsdokumentation für den Konnektor. Somit entspricht der TOE dem im Schutzprofil [BSI-CC-PP-0098] genannten Umfang und Aufbau.[1] Darüber hinaus entspricht der TOE auch dem im Schutzprofil für den Netzkonnektor definierten Funktionsumfang [BSI-CC-PP-0097].

1.3.1. TOE Typ

Die KoCoBox MED+ implementiert – konform zu [BSI-CC-PP-0098; BSI-CC-PP-0097] – den Produkttyp *Konnektor*.

1.3.2. Verwendung und Hauptfunktionalität des TOE

Der TOE ist eine sichere Komponente, die in der Telematikinfrastrukur als Konnektor eingesetzt wird. Die Funktionalität der KoCoBox MED+ geht aus der Konnektor-Spezifikation der gematik [gemSpec_Kon] hervor. Darüber hinaus finden weitere Spezifikationen der gematik Beachtung [gemSpec_Krypt]. Die Sicherheitsanforderungen spezifiziert das BSI in [BSI-CC-PP-0098; BSI-CC-PP-0097].

Die KoCoBox MED+ besteht aus ihrer Firmware (inklusive Betriebssystem und Anwendungssoftware) und der Hardwareplattform, einem herstellerspezifischen Design. Für die Zertifizierung wird nur die Firmware der KoCoBox MED+ betrachtet.

Die KoCoBox MED+ ist speziell entwickelt für Anwendungsfälle niedergelassener Ärzte, Kliniken und Apotheken.[2] Sie kann in IT-Umgebungen eingesetzt werden, die weitgehend ohne Administrator auskommen.

1.3.3. Erforderliche Non-TOE Hardware/Software/Firmware

Der TOE benötigt für den Betrieb verschiedene Komponenten. Als reiner Software-TOE muss die passende Hardware vorhanden sein. Der TOE ist auf die herstellereigene Hardware der KoCoBox MED+ angewiesen und kann nicht auf generischer Hardware betrieben werden.

Die kryptographischen Identitäten des Konnektors werden durch drei Smart Card basierte Sicherheitsmodule (gSMC-K) bereitgestellt, die in den internen Kartensteckplätzen des Konnektors installiert sind. Diese Smart Cards werden im Produktionsprozess eingebaut und sind nicht austauschbar. Weder Endbenutzer noch geschultes Service-Personal können die gSMC-K ersetzen. Die Manipulation oder das Entfernen der Smart Cards führt zur Außerbetriebssetzung des Geräts. Die Smart Cards sind nicht

[1] Allerdings sieht das Schutzprofil den Online-Rollout (Stufe 1) vor. Der TOE setzt einen neuen Stand der Spezifikation um.
[2] Im folgenden wird der Einfachheit halber angenommen, dass die Einsatzumgebung eine Arztpraxis ist.

Teil des TOE, sondern gehören zur Einsatzumgebung. Sie werden separat zertifiziert, vgl. [BSI-CC-PP-0082-2] und im Rahmen dieses Dokuments nicht weiter bewertet. Sowohl die Hardware als auch die gSMC-K gehören zum Lieferumfang der KoCoBox MED+.

1.4. Beschreibung des TOE

1.4.1. Hauptziele des TOE

Der Konnektor wurde als Bindeglied zwischen den Praxisverwaltungssystemen im LAN des Leistungserbringers und der Telematikinfrastruktur entwickelt. Der Konnektor setzt zwei Hauptziele um: Erstens stellt er eine sichere Verbindung zwischen den dezentralen und den zentralen Komponenten der Telematikinfrastruktur bereit; zweitens kontrolliert er die eHealth-Kartenterminals und Smart Cards, die eine fundamentale Rolle im Sicherheitskonzept der Telematikinfrastruktur spielen. Darüber hinaus implementiert der TOE verschiedene Fachanwendungen und eine Signaturanwendung. Der vorliegende TOE setzt *alle diese Ziele* um.

Sichere Verbindung in die Telematikinfrastruktur

Das erste Ziel ist, eine sichere Verbindung zur Telematikinfrastruktur bereitzustellen, die durch dynamische Paketfilter und Smart Card basiertes VPN abgesichert ist. Der Konnektor schützt sich selbst und die Telematikinfrastruktur vor Angriffen aus dem LAN des Leistungserbringers. Weiterhin schützt er die Komponenten im LAN vor Angriffen aus dem WAN.

Darüber hinaus stellt der Konnektor einen VPN-Tunnel zu einem sicheren Internetgateway (Secure Internet Service, SIS) zur Verfügung. Über diesen abgesicherten Internetzugang haben die Komponenten im LAN des Leistungserbringers einen abgesicherten und kontrollierten Zugang zum Internet, unter Umgehung des direkten WAN Zugangs über den DSL-Anschluss[3] der Praxis.

Kontrolle von Kartenterminals und Smart Cards

Das zweite Hauptziel ist, eine kontrollierte Verwendung der Aktoren im Umfeld der Telematikinfrastruktur zu ermöglichen. Die Aktoren in diesem Fall sind u. a. der Heilberufeausweis (HBA), die Institutionskarte (Smart Module Card-B, SMC-B) und die elektronische Gesundheitskarte (eGK). Doch auch die Smart Cards des Konnektors (vom Typ gSMC-K) enthalten kryptographische Identitäten für die Authentisierung und Identifikation gegenüber anderen Teilen der Infrastruktur: z. B. den VPN-Konzentratoren, eHealth-Kartenterminals und Clientsystemen. Darüber hinaus werden die Smart Cards auch zur Verschlüsselung und für Signaturen verwendet.

Signaturkomponente und Dokumentenverschlüsselung

Zusätzlich zu diesen Hauptzielen stellt der Konnektor noch eine Signaturerstellungskomponente bereit. Diese Komponente kann qualifizierte und nicht-qualifizierte elektronische Signaturen sowohl erzeugen als auch verifizieren. Der im Konnektor vorhandene Verschlüsselungsdienst kann von Produkten im LAN des Leistungserbringers verwendet werden, um Dokumente zu ver- und zu entschlüsseln. Das kryptographische Material, das in diese Prozesse eingeht, stammt von den Smart Cards, die der Konnektor kontrolliert.

[3] oder eine andere Zugangstechnologie

Abbildung 1.1.: Gehäuse der KoCoBox MED+

1.4.2. Aufbau des TOE

Der TOE ist ein reines Softwareprodukt. Er besteht aus der Firmware der KoCoBox MED+. Der Konnektor ist logisch aufgeteilt in zwei Bestandteile: Den Netzkonnektor (NK) und den Anwendungskonnektor (AK). Der Anwendungskonnektor enthält das Fachmodul VSDM. Die KoCoBox MED+ ist als eine Ein-Box Lösung ausgelegt. In der Spezifikation des Konnektors bezeichnet dieser Begriff ein Gerät, bei dem alle relevanten Komponenten in einem einzigen Gehäuse untergebracht sind. Das Gehäuse enthält sowohl den Netz-, als auch den Anwendungskonnektor. Das Gehäuse ist in Abbildung 1.1 dargestellt.

Das Gerät besteht neben der Software, die den TOE ausmacht, noch aus der Hardware. Die Hardware ist herstellerspezifisch. Die Software, die den TOE ausmacht, muss auf genau dieser Hardware betrieben werden. Der TOE benutzt die Hardware als Einsatzumgebung. Ebenso zur Einsatzumgebung gehören die drei im Gehäuse vorhandenen Smart Cards vom Typ gSMC-K. Die drei Secure Module Cards sind nicht Teil des TOE. Sie werden in diesem Security Target nicht beschrieben.

Das Betriebssystem der KoCoBox MED+ ist GNU/Linux. Teile des Betriebssystems setzen Sicherheitsanforderungen an den TOE um und sind somit SFR-enforcing. Das betrifft vor allem den TCP/IP-Stack, den Netfilter und das IPsec Protokoll. Der TOE ist in verschiedenen Programmiersprachen implementiert: C/C++, Shell-Skripte und Java.

Der Produkttyp und die Aufteilung der Funktionalität auf die einzelnen Systemkomponenten und

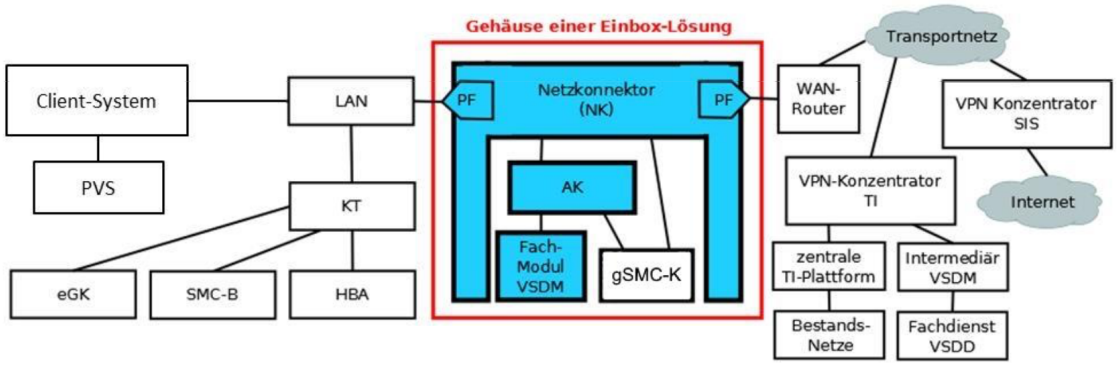


Abbildung 1.2.: Einsatzumgebung der KoCoBox MED+

die Funktionsblöcke werden in [BSI-CC-PP-0097; BSI-CC-PP-0098, Abschnitt 1.3.1] beschrieben.

1.4.3. Einsatzumgebung des TOE

Die Einsatzumgebung des TOE wird im Schutzprofil definiert [BSI-CC-PP-0098, Abschnitt 1.3.2]. Die dort gemachten Aussagen gelten ohne Anpassung für dieses Security Target. Die aus dem Schutzprofil übernommene Abbildung 1.2 zeigt die Einsatzumgebung des Konnektors.

Um die Telematikinfrastruktur gegen Angriffe aus dem LAN zu schützen, implementiert der TOE einen dynamischen Paketfilter, der auf beiden Ethernetschnittstellen (LAN und WAN) die ein- und ausgehenden Pakete überwacht. Derselbe Paketfilter schützt auch den TOE selbst, ebenfalls vor Angriffen aus dem LAN oder WAN.

Der Konnektor verbindet das LAN mit potenziell unsicheren Netzwerken wie dem Internet, die über das WAN Interface erreichbar sind. Der Konnektor stellt folglich das einzige Gateway des LAN ins WAN dar. [4]

Die Verbindung zwischen dem Konnektor und den gekoppelten eHealth Kartenterminals ist eine durch gegenseitige Authentisierung abgesicherte Verbindung.

Komponenten der Einsatzumgebung

Das sichere Funktionieren des Konnektors hängt vom Vorhandensein bestimmter Komponenten in der Einsatzumgebung ab. Solche Komponenten sind Hardware, Software und andere vertrauenswürdige IT-Produkte:

KoCoBox MED+ Hardware Der TOE als reines Softwareprodukt benötigt eine Hardware-Laufzeitumgebung, innerhalb derer die Programme des TOE ausgeführt werden können.

3 × STARCOS 3.6 Health SMCK R1 Vertrauenswürdige Smart Cards vom Typ gSMC-K mit der Zertifizierungs-ID BSI-DSZ-CC-0916-2015. Der Konnektor unterstützt drei Karten dieser Art, um die Performance bei kryptographischen Operationen zu steigern.

Telematikinfrastruktur Die TI wird von der gematik bereitgestellt. Sie ist für den TOE über das WAN Interface erreichbar. Die TI wird über die gematik Spezifikation „OPB 2.1“ definiert.

[4] Ausnahmen hiervon werden in der Konnektorspezifikation beschrieben [gemSpec_Kon, Anhang K]. In solchen Situationen – wie dort in Szenario 3 beschrieben – muss sichergestellt sein, dass das vorhandene Gateway abgesichert ist und nicht kompromittiert werden kann.

SIS Der sichere Internet-Service ist ein dedizierter VPN-Konzentrator, der über das WAN Interface des Konnektors erreichbar ist. Der SIS wird über die gematik Spezifikation „OPB 2.1“ definiert.

Web-Browser Der Konnektor wird über eine Web-Anwendung administriert. Diese Administratorschnittstelle erlaubt authentisierten Benutzern, verschiedene Management-Aufgaben zu erledigen. Diese Aufgaben sind z. B. das Einspielen aktueller Firmware, Anpassung der Konfigurationsparametern, und das Auslesen diagnostischer Informationen. Der Browser des Administrators gehört zur Einsatzumgebung und wird hier nicht bewertet. Die Verbindung eines Administrator-Arbeitsplatzes zu der Web-Anwendung ist immer über HTTPS abgesichert.

Clientsysteme Praxisverwaltungssysteme, die die Funktionen des Konnektors nutzen, müssen die Programmierschnittstellen des Konnektors befolgen [gemWSDL]. Die Anwendung dieser formalen Definition ist im Implementierungsleitfaden der gematik für Clientsysteme beschrieben [gemILF_PS].

Anforderungen an die Sicherheit der Einsatzumgebung

Der Konnektor soll in einem zutrittsgeschützten Bereich der Praxis betrieben werden und nur von vertrauenswürdigem und geschulten Personal benutzt werden. Daraus folgen einige Sicherheitsanforderungen an die Einsatzumgebung:

Identifikation eines physischen Angriffs Die Einsatzumgebung muss in der Lage sein, den Zugang eines Angreifers und die Manipulation an der Hardware des Geräts zu identifizieren.

Geschützter Betrieb Wenn das Gerät gestartet und betriebsbereit ist, muss die Einsatzumgebung den Zugang zum Konnektor verhindern. Das kann durch organisatorische, aber auch durch technische Maßnahmen erfolgen. Organisatorische Maßnahmen sind z. B. die regelmäßige Prüfung der Unversehrtheit des Betriebsraums; technische Maßnahmen sind z. B. die Installation einer Alarmanlage.

Befolgen anerkannter Sicherheitsregeln Regeln, die im IT-Grundschutz [BSI-GS] oder den Richtlinien der BÄK [BÄK-DV] formuliert sind, müssen angewendet werden.

1.4.4. Hardware der KoCoBox MED+

Abbildung 1.3 auf Seite 17 zeigt die Hardware-Komponenten, aus denen sich die Laufzeitumgebung des TOE zusammensetzt. Alle Teile des TOE werden durch die CPU des System-on-a-chip ausgeführt. Der TOE kann nicht auf anderen Hardware-Plattformen betrieben werden.

Die logischen Schnittstellen des TOE sind in dem Diagramm als von außen an die Systemkomponenten heranreichende Pfeile repräsentiert. Die entsprechenden physischen Schnittstellen sind in den äußeren Komponenten eingetragen. Die Real-Time-Clock (RTC) wird vom TOE verwendet, um zuverlässige Zeitstempel zu erzeugen. Die Uhr ist batteriegepuffert, um die korrekte Uhrzeit zu erhalten, wenn die KoCoBox MED+ vom Strom getrennt ist.

Die 2 GB RAM bilden den flüchtigen Arbeitsspeicher. Der persistente NAND-Flash Speicher befindet sich auf einer Speicherkarte (embedded Multimedia Card eMMC). Dieser Speicher ist 4 GB groß. Der 4 MB große NOR-Flash enthält den Bootloader.

Der duale Ethernet-Controller unterscheidet zwischen den zwei physischen Schnittstellen für das LAN (`PS.LAN`) und das WAN (`PS.WAN`). Für jede Schnittstelle wird ein eigener Port an der Außenseite

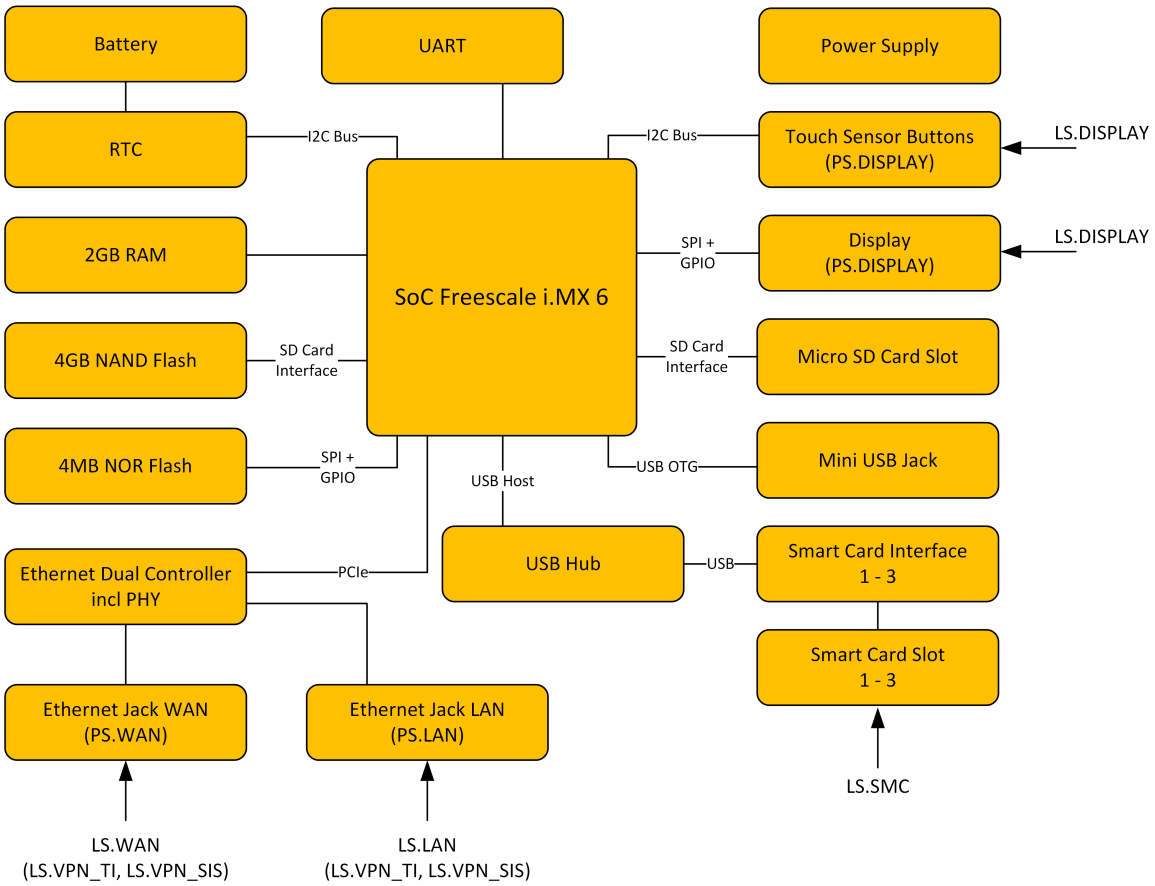


Abbildung 1.3.: Hardware-Komponenten der KoCoBox MED+

des Geräts angeboten. Jeder Port hat seine eigene MAC-Adresse. Der Controller erhält die Ethernet-Frames und ordnet die Frames dem jeweiligen Port zu. Der Controller stellt sicher, dass Frames nicht zwischen den Ports ausgetauscht weden. Basierend auf Port und MAC-Adresse bietet der TOE eindeutige Schnittstellen für jeden Port.

Die Tasten und das Display werden verwendet um Statusinformationen über die KoCoBox MED+ abzurufen. Weiterhin kann hierüber ein Neustart des Geräts ausgelöst werden.

Der Mini-USB Anschluss (USB On-the-Go, OTG) wird verwendet, um im Produktionsprozess die Firmware des Bootloader in die KoCoBox MED+ einzubringen. Für diesen Vorgang muss der SoC Pin für das Booten von USB-Medien während des Resets verbunden sein. Nur in diesem Fall handelt das SoC als ein USB-Gerät, sodass neue Firmware in den NOR-Flash Speicher geladen werden kann. Danach kann der Konnektor mit dem neuen Bootloader neugestartet werden. Der Pin am SoC ist eine interne Schnittstelle, deren Benutzung direkten Zugriff auf die Platine benötigt. Dieser Weg eine Firmware einzuspielen wird nur in der Fertigung verwendet und im Verlauf der Fertigung durch Fuses in der Hardware komplett deaktiviert. Somit ist sie während des Betriebs der KoCoBox MED+ nicht erreichbar. Als zusätzliche Schutzmaßnahme prüft der SoC vor dem Start die Signatur des Bootloader (High Assurance Boot, HAB). Danach werden durch weitere Verifizierungen von Signaturen zuerst der Kernel und das Initramfs und dann im Initramfs alle anderen Firmwareanteile auf ihre Integrität geprüft.

Der Micro SD-Kartenslot ist für zukünftige Anwendungszwecke vorgesehen. Er wird in der zertifizierten Konfiguration des TOE als alternatives Bootmedium verwendet. Der Kartenslot ist außerhalb des Geräts nicht zu erreichen.

Die UART-Schnittstelle zum Anschluss einer seriellen Konsole wird nicht benutzt. Sie ist über Software deaktiviert, sodass weder Eingaben noch Ausgaben darüber möglich sind.

1.4.5. Schnittstellen des Konnektors

1.4.5.1. Physische Schnittstellen

Alle Schnittstellen des Konnektors sind physisch am Gehäuse des Geräts untergebracht. Die folgende Liste bezieht sich auf die Liste der Schnittstellen, wie sie im Schutzprofil *des Gesamtkonnektors* [BSI-CC-PP-0098, Abschnitt 1.3.3.1] angegeben ist. Die Schnittstellen sind im Kontext der Systemarchitektur in Abbildung 1.3 aufgeführt, die außen sichtbaren Schnittstellen sind auf dem Foto des TOE in Abbildung 1.1 zu erkennen (vgl. Anwendungshinweis 5 des Schutzprofils).

Die Schnittstelle PS.DISPLAY ist zusätzlich aufgenommen. Hier erneut der Hinweis, dass der Evaluierungsgegenstand ein reines Softwareprodukt ist. Dennoch weist das Schutzprofil an, dass die physischen Außenschnittstellen des Geräts beschrieben werden sollen.

PS.LAN ist die Schnittstelle ins LAN und zu den Clientsystemen. Obwohl der Netzkonnektor selbst nicht direkt mit den Clientsystemen kommuniziert, stellt er die LAN-Schnittstelle zur Verfügung, die wiederum von Anwendungskonnektor verwendet wird, um mit Infrastruktur-Komponenten im LAN zu kommunizieren. Diese Schnittstelle stellt abhängig von der Konfiguration die Konnektivität für die VPN-Verbindungen in die TI und zum SIS zur Verfügung. Die Schnittstelle wird durch den Paketfilter des Netzkonnektors geschützt.

PS.WAN ist die Schnittstelle ins WAN. Diese Schnittstelle stellt abhängig von der Konfiguration die Konnektivität für die VPN-Verbindungen in die TI und zum SIS zur Verfügung. Die Schnittstelle wird durch den Paketfilter des Netzkonnektors geschützt.

PS.SMC ist die Schnittstelle zu den Smart Cards vom Typ gSMC-K, die im Konnektor fest verbaut sind. Die Schnittstelle verfügt über drei Steckplätze. Die Verwendung der jeweiligen Karten wird in Abschnitt 1.4.3 beschrieben.

PS.DISPLAY repräsentiert das Display und die Tasten an der Außenseite des Geräts. Das Display wird verwendet, um den Administrator über kritische Betriebszustände und den Verbindungsstatus zur TI und zum SIS zu informieren. Über die Tasten kann der Administrator durch ein Menü navigieren, um z. B. die Netzwerkparameter für das LAN abzulesen (keine Änderungsmöglichkeit) oder einen Neustart des Geräts auszulösen.

1.4.5.2. Logische Schnittstellen

Der TOE verfügt über die logischen Schnittstellen, die das Schutzprofil *des Gesamtkonnektors* [BSI-CC-PP-0098, Abschnitt 1.3.3.2] in beschreibt. Diese werden hier der besseren Lesbarkeit halber wiederholt.

LS.LAN ist die Schnittstelle ins lokale Netzwerk des Leistungserbringers. Zusätzlich zu den im Schutzprofil genannten Schnittstellen werden hier weitere protokollspezifische Schnittstellen definiert. Tabelle 1.1 listet diese Logischen Schnittstellen.

LS.WAN ist die Schnittstelle des TOE zum Internet Access Gateway (IAG). Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung des WAN. Tabelle 1.2 listet diese Logischen Schnittstellen.

LS.VPN_TI ist die Schnittstelle des TOE zu den zentralen Komponenten der Telematikinfrastruktur. Die Kommunikation erfolgt über einen VPN-Kanal, der über die WAN-Schnittstelle PS.WAN läuft. Ggf. läuft der VPN-Kanal alternativ über die Schnittstelle PS.LAN, falls WAN und LAN nicht getrennt sind. Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung des VPN_TI. Tabelle 1.3 listet diese Logischen Schnittstellen.

LS.VPN_SIS ist die Schnittstelle zum sicheren Internet Service SIS. Die Kommunikation erfolgt über einen VPN-Kanal, der über die WAN-Schnittstelle PS.WAN läuft. Ggf. läuft der VPN-Kanal alternativ über die Schnittstelle PS.LAN, falls WAN und LAN durch die Konfiguration des Konnektors über dieselbe Schnittstelle erreicht werden. Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung des VPN_SIS. Tabelle 1.4 listet diese Logischen Schnittstellen.

LS.SMC repräsentiert die logische Schnittstelle zum Sicherheitsmodul (gSMC-K) des Konnektors. Die Schnittstelle läuft über PS.SMC.

LS.DISPLAY repräsentiert die logische Schnittstelle zum Display und den Bedienknöpfen über PS.DISPLAY.

LS.FM ist die Schnittstelle zwischen dem Anwendungskonnektor und den Fachmodulen, die innerhalb des Konnektors laufen[5]. Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung der Fachmodule. Tabelle 1.5 listet diese Logischen Schnittstellen.

Die Funktionalität der Schnittstelle LS.FM.RMI wird detailreicher in Abschnitt 8.2 beschrieben.

[5] Das Fachmodul VSDM ist Teil des Anwendungskonnektors und verwendet diese Schnittstelle nicht.

Bezeichner	Rolle	Zweck der Schnittstelle
LS.LAN.CETP	Client	Übertragung von Systemereignissen an Clientsysteme
LS.LAN.DHCP	Server	Adressvergabe im LAN
LS.LAN.DNS	Server	Auflösung von Hostnamen im LAN
LS.LAN.Ether	—	Protokoll auf Zugangsschicht
LS.LAN.HTTP	Server	HTTP Zugriff auf Basisdienste
LS.LAN.HTTP_Client	Client	CRL Download
LS.LAN.HTTP.DVD	Server	Abruf des Dienstverzeichnis
LS.LAN.HTTP_MGMT	Server	HTTP-Zugriff auf Managementschnittstelle
LS.LAN.IP	—	Zugang zur Internet-Schicht
LS.LAN.IPsec	Client	Verbindung zu VPN-Konzentratoren, inkl. der Protokolle für Schlüsselaustausch und Verschlüsselung der Inhaltsdaten
LS.LAN.LDAP	Server	Zugriff auf den LDAP-Proxy
LS.LAN.NTP	Server	Abruf der Uhrzeit
LS.LAN.SICCT	Client	Kommunikation mit den eHealth-Kartenterminals
LS.LAN.SOAP	Server	SOAP Kommunikation mit den Basisdiensten
LS.LAN.SOAP.AuthSignatureService	Server	Zugriff auf den Authentisierungsdienst
LS.LAN.SOAP.CardService	Server	Zugriff auf den Kartendienst
LS.LAN.SOAP.CertificateService	Server	Zugriff auf den Zertifikatsdienst
LS.LAN.SOAP.CTService	Server	Zugriff auf den Kartenterminaldienst
LS.LAN.SOAP.EncryptionService	Server	Zugriff auf den Verschlüsselungsdienst
LS.LAN.SOAP.SignatureService	Server	Zugriff auf den Signaturdienst
LS.LAN.SOAP.SysInfService	Server	Zugriff auf den Systeminformationsdienst
LS.LAN.SOAP.VSDM	Server	Zugriff auf das Versichertenstammdatenmanagement
LS.LAN.SOAP.FM	Server	Zugriff auf die Fachmodule des Konnektors
LS.LAN.TCP	—	Zugang zur Transportschicht
LS.LAN.TLS	beide	Sicherung der Verbindung mit TLS 1.2
LS.LAN.UDP	—	Zugang zur Transportschicht

Tabelle 1.1.: Logische Schnittstellen an LS.LAN

Bezeichner	Rolle	Zweck der Schnittstelle
LS.WAN.DHCP	Client	Adressbezug im WAN
LS.WAN.DNS	Client	Auflösung von Hostnamen im WAN
LS.WAN.Ether	—	Protokoll auf Zugangsschicht
LS.WAN.HTTP_Client	Client	CRL Download
LS.WAN.IP	—	Zugang zur Internet-Schicht
LS.WAN.IPsec	Client	Verbindung zu VPN-Konzentratoren, inkl. der Protokolle für Schlüsselaustausch und Verschlüsselung der Inhaltsdaten
LS.WAN.SOAP	Client	SOAP Kommunikation mit dem Registrierungsdienst
LS.WAN.SOAP.RegService	Client	Registrieren des Konnektors am Registrierungsdienst
LS.WAN.TCP	—	Zugang zur Transportschicht
LS.WAN.TLS	Client	Sicherung der Verbindung mit TLS 1.2
LS.WAN.UDP	—	Zugang zur Transportschicht

Tabelle 1.2.: Logische Schnittstellen an LS.WAN

Bezeichner	Rolle	Zweck der Schnittstelle
LS.VPN_TI.DNS	Client	Auflösung von Hostnamen im WAN
LS.VPN_TI.HTTP	Client	HTTP Zugriff auf Fachdienste, Download der Updatepakete
LS.VPN_TI.HTTP_TSL	Client	TSL/CRL Download, OCSP Abfragen
LS.VPN_TI.IP	—	Zugang zur Internet-Schicht
LS.VPN_TI.LDAP	Client	Zugriff auf den Verzeichnisdienst der TI
LS.VPN_TI.SOAP	Client	SOAP Kommunikation mit den Fachdiensten VSDM
LS.VPN_TI.SOAP.VSDM	Client	Kommunikation mit den Fachdiensten VSDM
LS.VPN_TI.TCP	—	Zugang zur Transportschicht
LS.VPN_TI.TLS	Client	Sicherung der Verbindung mit TLS 1.2
LS.VPN_TI.UDP	—	Zugang zur Transportschicht

Tabelle 1.3.: Logische Schnittstellen an LS.VPN_TI

Bezeichner	Rolle	Zweck der Schnittstelle
LS.VPN_SIS.HTTP_Client	Client	TSL/CRL Download, HTTP Zugriff auf Fachdienste
LS.VPN_SIS.IP	—	Zugang zur Internet-Schicht
LS.VPN_SIS.TCP	—	Zugang zur Transportschicht
LS.VPN_SIS.UDP	—	Zugang zur Transportschicht

Tabelle 1.4.: Logische Schnittstellen an LS.VPN_SIS

Bezeichner	Rolle	Zweck der Schnittstelle
LS.FM.RMI	Server	RMI-Zugriffe der Fachmodule auf den Basiskonnektor
LS.FM.HTTP	Client	Durchleitung der HTTP-Zugriffe (SOAP-Requests) von Clientsystemen an die Fachmodule
LS.FM.HTTP_MGMT	Client	Durchleitung der HTTP-Zugriffe (Administration der Fachmodule) vom Browser des Administrators an die Fachmodule

Tabelle 1.5.: Logische Schnittstellen an LS.FM

1.4.6. Aufbau und physische Abgrenzung des Konnektors OPB 2.1

Das Schutzprofil verweist in [BSI-CC-PP-0098, Abschnitt 1.3.4] auf die Konzeption zur Architektur der TI-Plattform [gemKPT_Arch].

Das Betriebssystem, das der TOE bereit stellt, ist ein GNU/Linux System. Das im TOE verbaute Linux ist gegenüber der Basis-Distribution deutlich angepasst worden, sodass hier von einer eigenen Distribution gesprochen werden muss. Die Java-Anwendungen des TOE stellen die fachlichen Funktionen bereit. Der TOE besteht aus folgenden Subsystemen:

Bootloader Stellt die Integrität des Kernels und des Initramfs sicher; bootet den Kernel.

Kernel Der Kernel abstrahiert in Richtung der Anwendungen die Hardware und stellt Mechanismen für das Managemnt der Prozesse zur Verfügung. Der Kernel bietet Sicherheitsfunktionalität für den Paketfilter, die IPsec Kanäle und kryptographische Algorithmen.

Initramfs Enthält das initiale Dateisystem mit Tools und Skripten, die gebraucht werden, um nach dem Boot des Kernels das Root-Dateisystem zu laden.

Systemdienste in Form von Dämonen bieten Basisdienste, die von anderen Subsystemen des TOE genutzt werden.

Systembibliotheken und Werkzeuge Bietet Bibliotheken im User Space, Programme und Kommandozeilenwerkzeuge. Auch die Java Virtual Machine, in deren Instanzen der NK und der AK laufen, stammt aus diesem Subsystem. Programme im User Space tragen fachliche Funktionen wie Ver- und Entschlüsselung zum Gesamtsystem bei.

Skripte werden vor allem während des Systemstarts verwendet, um Systemdienste zu starten und den TOE zu konfigurieren.

JavaModule des NK Der in Java implementierte Teil des Netzkonnektors, der den TOE konfiguriert und anderen Teilen des TOE Dienste anbietet.

CertificateService Stellt anderen Subsystemen Funktionen zur Verifikation von Zertifikaten zur Verfügung.

RMIBridge Ermöglicht Funktionsaufrufe zwischen den beiden Java Virtual Machines des NK und des AK. Die Kommunikation kann in beide Richtungen erfolgen.

EventService Fungiert als eine interne Zentrale für die Verteilung von Ereignissen an andere Subsysteme und deren Module.

PCSCService Ermöglicht dem Anwendungskonnektor den Zugriff auf die im Konnektor verbauten Smart Cards vom Typ gSMC-K.

Facade Bildet aus Sicht der fachlich orientierten Subsysteme die technische Außenschnittstelle des Web-Servers ab.

FM_VSDM Dieses Subsystem stellt die Funktionen für das Versichertenstammdatenmanagemt bereit.

SystemInformationService Bietet Informationen über den Konnektor an. Nutzer sind sowohl interne Subsysteme (über ein Request-Reply Pattern), als auch Komponenten der Einsatzumgebung wie Clientsysteme (über ein Publish-Subscribe Pattern).

EncryptionService Bietet Ver- und Entschlüsselungsdienste für Clientsysteme und andere Subsysteme.

AdminService Enthält die Web-Application der Management-Schnittstelle und Basisdienste wie das User-Management und den Export/Import der Systemkonfiguration.

SignatureService Stellt Funktionen zum Signieren von Dokumenten und zur Verfikation von Signaturen zur Verfügung.

AccessAuthorizationService Setzt die Anforderungen an den Zugriffsschutz für Subsysteme des Anwendungskonnektors und das Informationsmodell um.

CardService Kapselt den Zugriff auf Smart Cards und eHealth-Kartenterminals; stellt anderen Subsystemen den Zugriff auf diese Entitäten zur Verfügung.

Tools.AK Bietet ein Sammelbecken für Programme, Werkzeuge und Frameworks, die von anderen Subsystemen herangezogen werden. Die prominentesten Vertreter sind das OSGi Framework als Modularisierungsplattform für Java-Anwendungen und das Krypto-Framework BouncyCastle.

LDAPProxy Stellt Funktionen bereit, damit Clientsysteme auf den Verzeichnisdienst der TI zugreifen können. Wird für die Kommunikation zwischen den Leistungserbringern verwendet.

AuthenticationService Bietet Authentisierungsmechanismen für Clientsysteme auf Basis der gematik Spezifikation zur Tokenbasierten Authentisierung [gemSpec_Kon_TBAuth]

Alle anderen Teile der KoCoBox MED+ gehören nicht zum TOE.

1.4.7. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste

1.4.7.1. Sicherheitsdienste des Netzkonnektors

Der Konnektor erfüllt alle Anforderungen an Sicherheitsdienste, die in [BSI-CC-PP-0098, Abschnitt 1.3.5.1] definiert werden. Die folgende Liste fasst die Sicherheitsdienste zusammen.

VPN Client um den Anwendungskonnektor mit den den zentralen Diensten der Telematikinfrastruktur und dem Sicheren Internet Service zu verbinden. Dabei werden insbesondere die im Folgenden dargestellten Funktionen umgesetzt

1. Erzwingen der Authentisierung des VPN Konzentrators. Der NK unterstützt IKEv2 gemäß [RFC 7296].
2. Schutz der Integrität und der Vertraulichkeit der übertragenen Daten.
3. Regelbasierte Informationsflusskontrolle.

Dynamischer Paketfilter Ein regelbasierter Paketfilter, der in der Lage ist, Angriffe mit hohem Potenzial aus LAN und WAN abzuwehren.

TLS-Basisdienst Die Java Virtual Machine, die Teil des Netzkonnektors ist, setzt über ihr Framework JSSE das TLS Protokoll im geforderten Maße um. Der TOE wird so konfiguriert, dass lediglich die in der gematik-Spezifikation genannten Ciphersuiten und Sicherheitsparameter verwendet werden können, vgl. [gemSpec_Krypt, Abschnitt 3.3.2].

Zeitdienst Bereitstellung eines NTP-Servers für Konnektor-interne Anwendungen wie das Audit-Log und für externe Komponenten wie Clientsysteme. Der NTP-Server synchronisiert sich mit den zentralen NTP-Servern der Telematikinfrastruktur.

Der NTP-Server prüft die erhaltenen Zeitinformationen auf Plausibilität und erlaubt keine Zeitabweichung über 3600 Sekunden hinaus.

DHCP-Dienst Systeme im LAN des Leistungserbringers können den DHCP-Server des Konnektors gemäß [RFC 2131; RFC 2132] nutzen.

DNS-Dienst Systeme im LAN des Leistungserbringers und der Anwendungskonnektor können den DNS-Server des Konnektors gemäß [RFC 4035] nutzen.

Gültigkeitsprüfung von Zertifikaten Der Konnektor validiert die Gültigkeit der Zertifikate, die von externen Entitäten wie den VPN-Konzentratoren zur Authentisierung präsentiert werden. Die Vertrauensanker für diese Prüfung werden aus der aktuell installierten TSL entnommen. Die verwendeten Algorithmen sind in der Firmware des Konnektors definiert und können durch Software-Updates aktualisiert werden.

Stateful Packet Inspection Der dynamische Paketfilter ist in der Lage, nicht-wohlgeformte IP-Pakete zu erkennen und entsprechend zu agieren.

Selbstschutz Der Konnektor schützt Geheimnisse gegen Manipulationen und Preisgabe.

Speicheraufbereitung Unmittelbar nach Abbau von TLS- und VPN-Verbindungen wird das Schlüsselmaterial durch aktives Überschreiben mit Null-Bytes vernichtet.

Selbsttests Neben dem beim Systemstart ausgeführten Selbsttest haben Administratoren jederzeit die Möglichkeit, den Selbsttest des Konnektors über die Management-Anwendung zu starten.

Protokollierung Der TOE reserviert Platz im nicht-flüchtigen Speicher für die Ablage eines Audit-Logs. Weder normale Benutzer noch Administratoren können das Audit-Log modifizieren oder löschen. Wenn der reservierte Speicherplatz erschöpft ist, wird der älteste Eintrag überschrieben.

Neben den in [BSI-CC-PP-0098, Abschnitt 6.2.5] beschriebenen Anforderungen werden noch die Anforderungen aus FAU_GEN.1/AK erfüllt.

Der TOE implementiert Mechanismen zum Selbstschutz gegen Angriffe, die das Audit-Log mit Einträgen zu überschwemmen versuchen, um Spuren eines Angriffs zu vertuschen. Bei einem Füllstand von 80% des Audit-Logs wird der Administrator über ein spezielles Audit-Event benachrichtigt.

Eine Auswertung des Audit-Logs ist Aufgabe des Administrators.

Administration Der TOE bietet eine web-basierte Management-Anwendung, die ausschließlich über eine TLS-gesicherte Verbindung erreichbar ist und die Authentisierung des Administrators über Benutzernamen/Passwort erzwingt. Diese Anwendung stellt der Anwendungskonnektor bereit. Die über die Management-Anwendung übergebenen Konfigurationswerte werden vom Netzkonnektor persistiert und angewendet.

Die Konfigurationsmöglichkeiten sind auf solche Werte beschränkt, die nicht die Sicherheitsanforderungen an den TOE gefährden. Die Sicherheit des TOE kann nicht durch Konfiguration in der Management-Anwendung kompromittiert werden.

Über die Management-Anwendung kann ein Administrator ein Firmware-Update initiieren.

Eine Fernwartung gemäß [gemSpec_Kon, Abschnitt 4.3] ist nicht möglich.

1.4.7.2. Sicherheitsdienste des Anwendungskonnektors

Die in [BSI-CC-PP-0098, Abschnitt 1.3.5.2] aufgeführten Sicherheitsdienste setzt der Anwendungskonnektor um. Für spezielle Sicherheitsdienste müssen die Anforderungen hier präzisiert werden:

Gesicherte Kommunikation Der Begriff „externes Managementsystem“ aus dem vierten Spiegelstrich wird hier als ein Signaturproxy interpretiert, der zwischen dem Clientsystem und dem TOE in der Einsatzumgebung vorhanden sein kann und über LS.LAN mit dem Konnektor kommuniziert.

TLS Dienst Die Anforderung

> Dazu dient der EVG als Proxy, der jeweils TLS-Kanäle zu Fachmodulen und zu Fachdiensten bzw. den vorgelagerten Intermediäre verwaltet [BSI-CC-PP-0098, S. 39]

wird in der vorliegenden Architektur nicht umgesetzt. Ein zentraler Dienst für die Verwaltung von TLS-Verbindungen existiert nicht. Jeder Nutzer einer TLS-Verbindung ist dafür verantwortlich, die Verbindung selbst auf- und wieder abzubauen. Das Framework JSSE stellt zwar alle Mechanismen für den Auf- und Abbau und für die Aufrechterhaltung einer TLS-Verbindung zur Verfügung, fungiert jedoch nicht als Manager der Verbindungen.

1.4.8. Physischer Umfang des TOE

Der physische Umfang des TOE umfasst die in Tabelle 1.6 aufgelisteten Komponenten.

Komponente	Beschreibung	Version
Firmware Image	Die Firmware und der Boot Loader des TOE. Die Firmware umfasst den Netzkonnektor, den Anwendungskonnektor, das Fachmodul NFDM (in Version 1.0.13) und das Fachmodul AMTS (Version 1.0.13)	2.3.24
Guidance Documentation („Administratorhandbuch KoCoBox MED+ Version 2.3“)	Die Guidance Documentation beschreibt die sichere Verwendung des TOE [KoCo AGD_ADM]	2.3 (14.7.2020)
Guidance Documentation („Ergänzungen zum Administratorhandbuch KoCoBox MED+ Version 2.x“)	Zielgruppe dieser Ergänzungen zum Handbuch sind Administratoren und Integratoren der KoCoBox MED+ sowie Hersteller von Primärsystemen, die für den Einsatz mit der KoCoBox MED+ vorgesehen sind. [KoCo AGD_ADM-Erg]	1.1.1
Benutzerhandbuch („Allgemeine Gebrauchsanleitung KoCoBox MED+“)	Das Benutzerhandbuch beschreibt die allgemeine Verwendung des Konnektors, sowohl dessen TOE Anteile als auch die nicht-TOE Anteile	1.3.8
Entwicklerhandbuch („JSON-Managementschnittstelle der KoCoBox MED+“)	Anleitung für die Benutzung der API von `LS.LAN.HTTP_MGMT`.	2.22
Konnektor Security Guidance Fachmodule NFDM und AMTS	Die Anleitung zur Verwendung des Konnektors für die Autoren von Fachmodulen AMTS und NFDM [KoCo AGD_KonSec]	1.15
Konnektor API für Fachmodule Javadoc	API-Beschreibung der Funktionen des Basiskonnektors für Fachmodule	2.3.24

Tabelle 1.6.: Physischer Umfang des TOE

2. Postulat der Übereinstimmung

2.1. Konformität zu Common Criteria

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

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

2.2. Konformität zu Schutzprofilen

Dieses Security Target behauptet strikte Konformität zu:

- „*Schutzprofil 2: Anforderungen an den Konnektor*“ [BSI-CC-PP-0098]

Dieses Security Target behauptet keine Konformität zu weiteren Schutzprofilen.

2.3. Konformität zu Paketen

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponenten in Tabelle 2.1. Dieses Security Target behauptet Konformität zu genau diesen Paketen. Diese Konformität wird als „EAL3+“ bezeichnet und ist somit „package-augmented“ gegenüber EAL3.

Paket	Erläuterung
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
ALC_FLR.2	Verfahren für Problemreports

Tabelle 2.1.: Ergänzungen zur Vertrauenswürdigkeit EAL3

2.4. Erklärung der Konformität

Dieses Security Target behauptet strikte Konformität zu [BSI-CC-PP-0098]. Durch diese Feststellung sind Widersprüche und Inkonsistenzen zu anderen Schutzprofilen ausgeschlossen. Diese Behauptung basiert auf der Betrachtung des TOE Typs, der Definition des Sicherheitsproblems und schließlich

der Sicherheitsziele sowie der Sicherheitsanforderungen. Weiterhin behauptet dieses Security Target Konformität zu allen Security Assurance Requirements (SARs), die von [BSI-CC-PP-0098] gefordert werden.

TOE Typ Das Schutzprofil fordert, dass der TOE ein *Konnektor* gemäß der Spezifikation der gematik ist [gemSpec_Kon]. Der TOE, der in diesem Security Target beschrieben wird, ist ein solcher Konnektor. Er besteht aus dem Netzkonnektor, dem Anwendungskonnektor und dem Fachmodul „Versichertenstammdatenmanagement“.

Definition des Sicherheitsproblems Die Definition des Sicherheitsproblems, d. h. die Bedrohungen, Annahmen und die organisatorischen Sicherheitspolitiken sind direkt aus dem Schutzprofil [BSI-CC-PP-0098] übernommen.

Sicherheitsziele und Sicherheitsanforderungen Die Sicherheitsziele und Sicherheitsanforderungen sind dem Schutzprofil [BSI-CC-PP-0098] entnommen. Die Operationen an den SFR sind deutlich gekennzeichnet.

Kapitel 5 bescheibt die über CC Teil 2 [CC Part 2] hinausgehenden funktionalen Anforderungen an die Vertrauenswürdigkeit. Es werden keine Anforderungen definiert, die über CC Teil 3 [CC Part 3] hinausgehen.

2.5. Konformität zu Technischen Richtlinien für Fachmodule

Dieses Security Target ist weiterhin konform zu den Anforderungen, die folgende Technische Richtlinien an einen CC-zertifizierten Konnektor stellen:

- „*Konnektor – Prüfspezifikation für das Fachmodul NFDM*“ [TR-03154, Abschnitt 3.3.2]
- „*Konnektor – Prüfspezifikation für das Fachmodul AMTS*“ [TR-03155, Abschnitt 3.3.2]

Die Konformitätserklärung zu den Technischen Richtlinien bedeutet *nicht*, dass der Konnektor die gesamte TR umsetzt. Sie bezieht sich ausschließlich auf die Anforderungen an die CC-Zertifizierung in den angegebenen Abschnitten der Technischen Richtlinien. Die Erklärung der Konformität folgt in Kapitel 8.

3. Definition des Sicherheitsproblems

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

Für die Bezüge auf Schutzprofile sind die Hinweise im Abschnitt „Anmerkungen zur CC Zertifizierung“ im Vorwort dieses Security Targets zu beachten.

3.1. Werte

3.1.1. Zu Schützende Werte

Die *zu schützenden Werte* – also Ressourcen und Daten, die der TOE schützt – werden in [BSI-CC-PP-0097] und [BSI-CC-PP-0098] beschrieben. Die dort beschriebenen Werte gelten bezüglich des TOE Scopes ohne Anpassung, vgl. hierzu auch die Anmerkungen im Vorwort dieses Security Targets.

3.1.2. Benutzer des TOE

Die *externen Entitäten, Subjekte und Objekte* des TOE werden in [BSI-CC-PP-0097] und [BSI-CC-PP-0098] beschrieben. Die *Benutzer* des Anwendungskonnektors werden in [BSI-CC-PP-0098, Abschnitt 3.1.1] beschrieben. Diese Beschreibung gilt ohne Anpassung. Die Subjekte, die im Auftrag des Benutzers agieren, werden in [BSI-CC-PP-0098, Abschnitt 6.1.2] modelliert. Auch diese Darstellung wird ohne Anpassung in das Security Target übernommen.

3.2. Bedrohungen

Die in [BSI-CC-PP-0097] und in den [BSI-CC-PP-0098] aufgelisteten und angenommenen *Bedrohungen* gelten bezüglich des TOE Scopes ohne Anpassung, vgl. hierzu auch die Anmerkungen im Vorwort dieses Security Targets.

3.3. Organisatorische Sicherheitspolitiken des Netzkonnektors

OSP.NK.Zeitdienst (Zeitdienst)
Die in Abschnitt 3.4 von [BSI-CC-PP-0097] und Abschnitt 3.3.1 von [BSI-CC-PP-0098] beschriebene organisatorische Sicherheitspolitik OSP.NK.Zeitdienst gilt ohne Anpassung.

OSP.NK.SIS (Sicherer Internet Service)
Die in Abschnitt 3.4 von [BSI-CC-PP-0097] und Abschnitt 3.3.1 von [BSI-CC-PP-0098] beschriebene organisatorische Sicherheitspolitik OSP.NK.SIS gilt ohne Anpassung.

OSP.NK.BOF (Kommunikation mit Bestandsnetzen und offenen Fachdiensten)
Die in Abschnitt 3.4 von [BSI-CC-PP-0097] und Abschnitt 3.3.1 von [BSI-CC-PP-0098] beschriebene organisatorische Sicherheitspolitik OSP.NK.BOF gilt ohne Anpassung.

OSP.NK.TLS (TLS-Kanäle mit sicheren kryptographische Algorithmen)
Die in Abschnitt 3.4 von [BSI-CC-PP-0097] und Abschnitt 3.3.1 von [BSI-CC-PP-0098] beschriebene organisatorische Sicherheitspolitik OSP.NK.TLS gilt ohne Anpassung.

3.4. Organisatorische Sicherheitspolitiken des Anwendungskonnektors

Die in [BSI-CC-PP-0098, Abschnitt 3.3] aufgelisteten *organisatorischen Sicherheitspolitiken* gelten ohne Anpassung.

3.5. Annahmen

Die in [BSI-CC-PP-0097] und [BSI-CC-PP-0098] getroffenen *Annahmen* gelten bezüglich des TOE Scopes ohne Anpassung, vgl. hierzu auch die Anmerkungen im Vorwort dieses Security Targets.

Für A.NK.AK und A.NK.CS wird der ST-Autor über Anwendungshinweise Nr. 28 und 29 aufgefordert, die Funktionalität des Netzkonnektors und die dafür erforderlichen Separationsmechanismen zu erklären. Zwar gehen die beiden Annahmen davon aus, dass sowohl der Anwendungskonnektor als auch die Clientsysteme die Sicherheitsdienste des Netzkonnektors automatisch nutzen. Doch muss auch aus dem LAN des Leistungserbringers mit Angriffen gerechnet werden, da möglicherweise Schadsoftware im LAN existiert. Dies leitet sich aus zwei Bedrohungen her, denen das Schutzprofil verschiedene Angriffspfade zuordnet [BSI-CC-PP-0098, Abschnitt 3.2.1.2].

T.NK.local_EVG_LAN Die in Angriffspfad 1 skizzierte Gefahr kann für den Konnektor ausgeschlossen werden. Der Konnektor verwendet an der LAN Schnittstelle einen Paketfilter, der nicht umgangen werden kann. Außer den definierten Schnittstellen sind keine Ports am Konnektor geöffnet. Daher gelten hier die üblichen Schutzmaßnahmen wie der Integritätsschutz.

Die im Konnektor eingetragenen Routing-Tabellen sorgen dafür, dass Clientsysteme direkt mit den angeschlossenen Netzen des Gesundheitswesens („offene Bestandsnetze“) kommunizieren dürfen.

T.NK.remote_EVG_LAN Der Paketfilter separiert auch die Schnittstellen LS.LAN und LS.WAN voneinander. Weiterhin haben LAN- und WAN-Interfaces unterschiedliche IP-Adressen. Sie arbeiten in unterschiedlichen Subnetzen, diese dürfen sich nicht überschneiden. Folglich separiert auch das Routing die beiden Netze. Damit ist der Angriffspfad 3.1 abgewehrt. Der Angriffspfad 3.2 muss durch das Clientsystem abgewehrt werden.

In beiden Fällen werden vor allem Inhalte der Kommunikation nicht ausgewertet: Der Konnektor ist ja nur angreifbar, wenn auf dem Konnektor irgendetwas zur Auswertung ankommt. Firewall und Routing selber werten ja nur die Pakete auf IP/TCP/UDP Ebene aus. Der Konnektor fungiert in diesem Fall lediglich als Router, der weder den Anspruch erhebt, noch in der Lage ist, den von ihm an die Clientsysteme vermittelten Datenverkehr zu überwachen und zu filtern. Dienste auf dem Konnektor selber sind erreichbar und müssen sich selber schützen bzw sind auf anderen Ebenen separiert.

4. Sicherheitsziele

4.1. Sicherheitsziele für den Netzkonnektor

4.1.1. Allgemeine Ziele: Schutz und Administration

O.NK.TLS_Krypto (TLS-Kanäle mit sicheren kryptographische Algorithmen)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.TLS_Krypto muss erfüllt werden.

O.NK.Schutz (Selbstschutz, Selbsttest und Schutz von Benutzerdaten)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Schutz muss erfüllt werden.

O.NK.EVG_Authenticity (Authentizität des EVG)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.EVG_Authenticity muss erfüllt werden.

Einen hinreichenden Schutz gegen Angreifer, welche gefälschte Konnektoren in Umlauf bringen, stellen ein geeignetes Auslieferungsverfahren (ALC_DEL.1) sowie sichere Verfahren zur Inbetriebnahme (AGD_OPE.1) dar, sofern sie mit weiteren Maßnahmen kombiniert werden, welche spätere Veränderungen am Konnektor mit Sicherheit ausschließen oder hinreichend erkennbar machen, z. .B. Aufbewahrung in einem gesicherten Bereich (siehe Abschnitt 4.1.1).

Der Konnektor wird über ein sicheres Auslieferungsverfahren an den Bestimmungsort transportiert und dort dem Leistungserbringer übergeben. Die Eigenschaften des sicheren Auslieferungsprozess sind in [KoCo ALC_DEL] beschrieben. Das Administratorhandbuch listet in Abschnitt 4.2 die Art und die Plazierung der verschiedenen Siegel auf dem Gehäuse des Konnektors auf [KoCo AGD_ADM]. Anhand der Unversehrtheit der Siegel ist für den Leistungserbringer erkennbar, ob das Gerät manipuliert wurde.

Der Konnektor implementiert das IPSec-Protokoll, das eine zertifikatsbasierte Authentisierung vorsieht. Das Zertifikat bezieht der Konnektor von der gSMC-K#1. Diese Karte ist im Konnektor verbaut und kann nicht entfernt werden, ohne die Integrität des Konnektors zu zerstören.

O.NK.Admin_EVG (Administration nur nach Autorisierung und über sicheren Kanal)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Admin_EVG muss erfüllt werden.

Das Administrationskonzept des Konnektors ist rollenbasiert, doch jeder Benutzer mit der Berechtigung, die Administrationsschnittstelle zu benutzen, wird in diesem Security Target als Administrator bezeichnet – unabhängig von den konfigurierten Berechtigungen der spezifischen Rolle. Das Rollenmodell des Konnektors weist weitere Rollen auf (*SuperAdmin*, *Admin* etc., vgl. [KoCo AGD_ADM]), die mit verschiedenen Rechten versehen sind und durch Einzelvergabe individuell konfiguriert werden können. Aus Sicht dieses Security Targets werden die Inhaber dieser Rollen alle als „Administrator“ bezeichnet.

O.NK.Protokoll (Protokollierung mit Zeitstempel)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Protokoll muss erfüllt werden.

O.NK.Zeitdienst (Zeitdienst)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-0097] und Abschnitt 4.1.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Zeitdienst muss erfüllt werden.

4.1.2. Ziele für die VPN Funktionalität

O.NK.VPN_Auth (Gegenseitige Authentisierung im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-0097] und Abschnitt 4.1.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.VPN_Auth muss erfüllt werden.

O.NK.Zert_Prüf (Gültigkeitsprüfung für VPN-Zertifikate)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-0097] und Abschnitt 4.1.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Zert_Prüf muss erfüllt werden.

O.NK.VPN_Vertraul (Schutz der Vertraulichkeit von Daten im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-0097] und Abschnitt 4.1.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.VPN_Vertraul muss erfüllt werden.

O.NK.VPN_Integrität (Integritätsschutz von Daten im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-0097] und Abschnitt 4.1.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.VPN_Integrität muss erfüllt werden.

4.1.3. Ziele für die Paketfilter-Funktionalität

O.NK.PF_WAN (Dynamischer Paketfilter zum WAN)
Das in Abschnitt 4.1.3 von [BSI-CC-PP-0097] und Abschnitt 4.1.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.PF_WAN muss erfüllt werden.

O.NK.PF_LAN (Dynamischer Paketfilter zum LAN)
Das in Abschnitt 4.1.3 von [BSI-CC-PP-0097] und Abschnitt 4.1.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.PF_LAN muss erfüllt werden.

O.NK.Stateful (Stateful Packet Inspection (zustandsgesteuerte Filterung))
Das in Abschnitt 4.1.3 von [BSI-CC-PP-0097] und Abschnitt 4.1.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.NK.Stateful muss erfüllt werden.

4.2. Sicherheitsziele für den Anwendungskonnektor

4.2.1. Allgemeine Sicherheitsziele

O.AK.Basis_Crypto (Kryptographische Algorithmen)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Basis_Crypto muss erfüllt werden.

O.AK.Admin (Administration)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Admin muss erfüllt werden.

O.AK.EVG_Modifikation (Schutz vor Veränderungen)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.EVG_Modifikation muss erfüllt werden.

O.AK.Selbsttest (Selbsttests)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Selbsttest muss erfüllt werden.

O.AK.Protokoll (Sicherheitsprotokoll mit Zeitstempel)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Protokoll muss erfüllt werden.

O.AK.Zeit (Systemzeit)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Zeit muss erfüllt werden.

O.AK.Infomodell (Umsetzung des Informationsmodells durch den EVG)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Infomodell muss erfüllt werden.

O.AK.Update (Software Update und Update von TSL, CRL und BNetzA-VL)
Das in Abschnitt 4.2.1 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Update muss erfüllt werden.

4.2.2. Signaturdienst

O.AK.Sig.SignQES (Signaturrichtlinie für qualifizierte elektronische Signaturen)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.SignQES muss erfüllt werden.

O.AK.Sig.SignNonQES (Signaturrichtlinie für nichtqualifizierte elektronische Signaturen)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.SignNonQES muss erfüllt werden.

O.AK.Sig.exklusivZugriff (Unterstützung bei alleiniger Kontrolle)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.exklusivZugriff muss erfüllt werden.

O.AK.Sig.Einfachsignatur (Einfachsignatur)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.Einfachsignatur muss erfüllt werden.

O.AK.Sig.Stapelsignatur (Stapelsignatur)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.Stapelsignatur muss erfüllt werden.

O.AK.Sig.Schlüsselinhaber (Zuordnung des Signaturschlüssel-Inhabers)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.Schlüsselinhaber muss erfüllt werden.

O.AK.Sig.SignaturVerifizierung (Verifizierung der Signatur)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.SignaturVerifizierung muss erfüllt werden.

O.AK.Sig.PrüfungZertifikat (Prüfung des Signatur-Zertifikates)
Das in Abschnitt 4.2.2 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Sig.PrüfungZertifikat muss erfüllt werden.

4.2.3. Gesicherte Kommunikation / TLS Proxy

O.AK.LAN (gesicherte Kommunikation im LAN der Leistungserbringer)
Das in Abschnitt 4.2.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.LAN muss erfüllt werden.

O.AK.WAN (gesicherte Kommunikation zwischen EVG und Fachdiensten)
Das in Abschnitt 4.2.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.WAN muss erfüllt werden.

4.2.4. Terminal- und Chipkartendienst

O.AK.exklusivZugriff (Alleinige Kontrolle von Terminal und Karte)
Das in Abschnitt 4.2.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.exklusivZugriff muss erfüllt werden.

O.AK.PinManagement (Management von Chipkarten-PINs)
Das in Abschnitt 4.2.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.PinManagement muss erfüllt werden.

O.AK.IFD-Komm (Schutz der Kommunikation mit den eHealth-Kartenterminals)
Das in Abschnitt 4.2.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.IFD-Komm muss erfüllt werden.

O.AK.Chipkartendienst (Chipkartendienste des EVG)
Das in Abschnitt 4.2.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Chipkartendienst muss erfüllt werden.

O.AK.VAD (Schutz der Authentisierungsverifikationsdaten)
Das in Abschnitt 4.2.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.VAD muss erfüllt werden.

4.2.5. Verschlüsselungsdienste

O.AK.Enc (Verschlüsselung von Daten)
Das in Abschnitt 4.2.5 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Enc muss erfüllt werden.

O.AK.Dec (Entschlüsselung von Daten)
Das in Abschnitt 4.2.5 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.Dec muss erfüllt werden.

O.AK.VZD (Kommunikation mit dem zentralen Verzeichnisdienst)
Das in Abschnitt 4.2.5 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.VZD muss erfüllt werden.

4.2.6. Fachmodul VSDM

O.AK.VSDM (Versichertenstammdatenmanagement)
Das in Abschnitt 4.2.5 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel O.AK.VSDM muss erfüllt werden.

4.3. Sicherheitsziele für die Umgebung des Netzkonnektors

OE.NK.RNG (Externer Zufallszahlengenerator)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.RNG muss erfüllt werden.

OE.NK.Echtzeituhr (Echtzeituhr)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Echtzeituhr muss erfüllt werden.

OE.NK.Zeitsynchro (Zeitsynchronisation)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Zeitsynchro muss erfüllt werden.

OE.NK.gSMC-K (Sicherheitsmodul gSMC-K)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.gSMC-K muss erfüllt werden.

OE.NK.KeyStorage (Sicherer Schlüsselspeicher)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.KeyStorage muss erfüllt werden.

OE.NK.AK (Korrekte Nutzung des EVG durch Anwendungskonnektor)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.AK muss erfüllt werden.

OE.NK.CS (Korrekte Nutzung des Konnektors durch Clientsysteme (oder weitere Systeme im LAN))
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.CS muss erfüllt werden.

OE.NK.Admin_EVG (Sichere Administration des EVG)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Admin_EVG muss erfüllt werden.

OE.NK.Admin_Auth (Authentisierung des Administrators)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Admin_Auth muss erfüllt werden.

OE.NK.PKI (Betrieb einer Public-Key-Infrastruktur und Verteilung der TSL)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.PKI muss erfüllt werden.

OE.NK.phys_Schutz (Physischer Schutz des EVG)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.phys_Schutz muss erfüllt werden.

OE.NK.sichere_TI (Sichere Telematikinfrastruktur Platform)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.sichere_TI muss erfüllt werden.

OE.NK.kein_DoS (Keine Denial Of Service Angriffe)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.kein_DoS muss erfüllt werden.

OE.NK.Betrieb_AK (Sicherer Betrieb des Anwendungskonnektors)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Betrieb_AK muss erfüllt werden.

OE.NK.Betrieb_CS (Sicherer Betrieb der Clientsysteme)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Betrieb_CS muss erfüllt werden.

OE.NK.Ersatzverfahren (Sichere Ersatzverfahren bei Ausfall der Infrastruktur)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.Ersatzverfahren muss erfüllt werden.

OE.NK.SIS (Sicherer Internet Service)
Das in Abschnitt 4.2 von [BSI-CC-PP-0097] und Abschnitt 4.3 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.NK.SIS muss erfüllt werden.

4.4. Sicherheitsziele für die Umgebung des Anwendungskonnektors

OE.AK.Versicherter (Sorgfaltspflichten des Versicherten)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Versicherter muss erfüllt werden.

OE.AK.HBA-Inhaber (Vertrauenswürdigkeit und Sorgfaltspflichten des HBA-Inhabers)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.HBA-Inhaber muss erfüllt werden.

OE.AK.SMC-B-PIN (Freischaltung der SMC-B)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.SMC-B-PIN muss erfüllt werden.

OE.AK.sichere_TI (Sichere Telematikinfrastruktur-Plattform)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.sichere_TI muss erfüllt werden.

OE.AK.Fachdienste (Vertrauenswürdige Fachdienste und zentrale Dienste der TI-Plattform)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Fachdienste muss erfüllt werden.

OE.AK.Admin_EVG (Sichere Administration des Konnektors)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Admin_EVG muss erfüllt werden.

OE.AK.Admin_Konsole (Sichere Administratorkonsole)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Admin_Konsole muss erfüllt werden.

OE.AK.Kartenterminal (Sicheres Kartenterminal)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Kartenterminal muss erfüllt werden.

OE.AK.Plattform (Sichere Plattform)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Plattform muss erfüllt werden.

OE.AK.SecAuthData (Schutz der Authentisierungsdaten)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.SecAuthData muss erfüllt werden.

OE.AK.phys_Schutz (Physischer Schutz des EVG)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.phys_Schutz muss erfüllt werden.

OE.AK.Personal (Qualifiziertes und vertrauenswürdiges Personal)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Personal muss erfüllt werden.

OE.AK.SMC (Nutzung geeigneter SMC)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.SMC muss erfüllt werden.

OE.AK.gSMC-K (Nutzung einer gSMC-K)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.gSMC-K muss erfüllt werden.

OE.AK.eGK (Nutzung geeigneter eGK)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.eGK muss erfüllt werden.

OE.AK.HBA (Nutzung einer sicheren Signaturerstellungseinheit)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.HBA muss erfüllt werden.

OE.AK.PKI (PKI für Signaturdienste, Verschlüsselung und technische Komponenten)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.PKI muss erfüllt werden.

OE.AK.Clientsystem (Sichere Clientsysteme)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Clientsystem muss erfüllt werden.

OE.AK.ClientsystemKorrekt (Clientsysteme arbeiten korrekt und unterstützen das Informationsmodell)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.ClientsystemKorrekt muss erfüllt werden.

OE.AK.Benutzer_Signatur (Prüfung zu signierender und zu prüfender Dokumente vor der Übermittlung an den EVG)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Benutzer_Signatur muss erfüllt werden.

OE.AK.SW-Update (Prozesse für sicheres Software-Update)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.SW-Update muss erfüllt werden.

OE.AK.Echtzeituhr (Bereitstellung einer Echtzeituhr)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Echtzeituhr muss erfüllt werden.

4.5. Erklärung der Sicherheitsziele des Netzkonnektors

4.5.1. Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele

Die Abbildung der Bedrohungen, organisatorischen Sicherheitspolitiken und Annahmen auf Sicherheitsziele für den TOE entspricht den in [BSI-CC-PP-0098; BSI-CC-PP-0097] beschriebenen Relationen. Tabelle 4.1 entspricht der Übersicht im Schutzprofil. Tabelle A.1 zeigt die in Tabelle 4.1 verwendeten Symbole.

Das Schutzprofil beschreibt darüber hinaus, dass einige Bedrohungen durch Assurance-Komponenten der CC abgewehrt werden. Diese zusätzliche Sicherung gilt auch für dieses Security Target.

4.5.1.1. Abwehr der Bedrohungen durch die Sicherheitsziele

Die Verteidigung gegen Bedrohungen, die im Schutzprofil definiert werden, werden unverändert aus dem Schutzprofil übernommen.

	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	.	✓	.	.	✓	✓	.	.	.	.	.	✓	–	.	✓	✓	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
T.NK.remote_EVG_WAN	.	✓	.	.	✓	✓	✓	✓	.	✓	✓	.	✓	✓	✓	✓	✓	✓	.	.	.	.	✓	.	✓	.	.	.	✓	.
T.NK.remote_EVG_LAN	.	✓	.	.	✓	✓	✓	✓	.	✓	✓	✓	✓	✓	✓	✓	✓	✓	.	.	.	.	✓	.	✓	.	.	✓	✓	✓
T.NK.remote_VPN_Data	.	.	.	–	✓	✓	✓	✓	✓	.	.	.	✓	✓	✓	✓	✓	✓	✓	.	.	.	✓	.	✓	.	✓	✓	✓	✓
T.NK.local_admin_LAN	.	✓	.	✓	✓	✓	.	.	.	.	.	–	–	✓	✓	✓	.	✓	.	.	✓	✓	–	–	.	.	.	.	–	.
T.NK.remote_admin_WAN	.	✓	.	✓	✓	✓	.	.	.	.	–	.	–	✓	✓	✓	.	✓	.	.	✓	✓	–	.	.	.	.	.	–	.
T.NK.counterfeit	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	✓	.	.	.	.	✓	.
T.NK.Zert_Prüf	.	.	.	.	–	–	.	✓	.	.	–	.	–	–	–	–	–	.	.	.	.	.	✓	.	.	.	.	.	✓	.
T.NK.TimeSync	.	.	.	.	–	✓	✓	✓	.	✓	–	.	–	✓	✓	✓	✓	.	.	.	.	.	✓	.	.	.	.	.	✓	.
T.NK.DNS	.	.	.	.	–	–	✓	✓	.	.	–	.	–	.	–	–	.	.	.	.	.	.	✓	.	.	.	.	✓	✓	–
OSP.NK.Zeitdienst	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	✓	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
OSP.NK.SIS	.	.	.	.	.	.	.	.	.	.	✓	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
OSP.NK.BOF	.	.	.	.	.	.	✓	✓	✓	✓	✓	.	✓	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
OSP.NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
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	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
A.NK.Ersatzverfahren	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
A.NK.Zugriff_gSMC-K	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	✓	.	.	.

Tabelle 4.1.: Abbildung der Sicherheitsziele des Netzkonnektors auf Bedrohungen und Annahmen

4.5.1.2. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

Die Abbildungen der organisatorischen Sicherheitspolitiken OSP.NK.Zeitdienst, OSP.NK.SIS, OSP.NK.BOF und OSP.NK.TLS auf Sicherheitsziele wird unverändert aus dem Schutzprofil übernommen.

4.5.1.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Die Abbildung der Annahmen auf Sicherheitsziele der Umgebung wird unverändert aus dem Schutzprofil übernommen.

4.6. Erklärung der Sicherheitsziele des Anwendungskonnektors

Die Erklärung der Sicherheitsziele und die Zuordnung zu Bedrohungen, Sicherheitspolitiken und Annahmen wird ohne Änderung aus dem Schutzprofil übernommen [BSI-CC-PP-0098, Abschnitt 4.5].

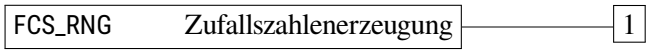
5. Definition der erweiterten Komponenten

5.1. Definition der erweiterten Familie FCS_RNG

Familienverhalten

Diese Familie definiert Anforderungen an die Erzeugung von Zufallszahlen, die für kryptographische Anwendungen vorgesehen sind.

Komponentenabstufung



FCS_RNG.1 „Zufallszahlenerzeugung“ erfordert die Identifizierung des Typs des verwendeten Zufallszahlengenerators und eine Auflistung seiner Sicherheitsmerkmale. Für die erzeugten Zufallszahlen ist eine Qualitätsmetrik anzugeben, auf die sich ihre nachfolgende Verarbeitung und Bewertung abstützen kann.

Management: FCS_RNG.1

Für diese Komponente sind keine Management-Aktivitäten vorgesehen.

Protokollierung: FCS_RNG.1

Es sind keine Ereignisse identifiziert, die protokollierbar sein sollen, wenn FAU_GEN Generierung der Sicherheitsprotokolldaten Bestandteil des PP/des ST ist.

FCS_RNG.1
Zufallszahlenerzeugung

Hierarchical to:	Keine andere Komponente
Dependencies:	Keine Abhängigkeiten
FCS_RNG.1.1	The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Erklärung für die Einführung der erweiterten Familie

Laut der Definition von OE.NK.RNG in [BSI-CC-PP-0098; BSI-CC-PP-0097] ist die Umgebung des Konnektors für die Zulieferung von Zufallszahlen verantwortlich. Dabei wird nahegelegt, dass die gSMC-K verwendet werden soll:

> Es ist vorgesehen, den Zufallszahlengenerator der gSMC-K als physikalischen Zufallszahlengenerator der Klasse PTG.2 zu nutzen.

Die KoCoBox MED+ verwendet den Zufallsgenerator der gSMC-K; allerdings wird er genutzt, um einen eigenen Zufallsgenerator Hash_DRBG nach [NIST SP 800-90A, Sect. 10.1.1] in regelmäßigen Abständen mit Zufallszahlen zu initialisieren. Um die Sicherheitseigenschaften dieser eigenen Implementierung beschreiben zu können, wird hier die Familie FCS_RNG eingeführt. Deren SFR werden später benutzt, um Anforderungen an den Zufallsgenerator des TOE zu stellen.

5.2. Definition der erweiterten Familie FPT_EMS

Die Definitionen der Familie FPT_EMS und der Sicherheitsanforderung FPT_EMS.1 werden ohne Änderung aus [BSI-CC-PP-0097] und [BSI-CC-PP-0098] übernommen.

5.3. Definition der erweiterten Familie FIA_API

Die Definitionen der Familie FIA_API und der Sicherheitsanforderung fia_api.1/ak werden ohne Änderung aus [BSI-CC-PP-0098] übernommen.

6. Sicherheitsanforderungen

6.1. Hinweise und Definitionen

Der größte Teil der Sicherheitsanforderungen wird ohne Anpassungen aus dem Schutzprofil übernommen. Anpassungen werden kenntlich gemacht. Bei denjenigen SFR, die das Schutzprofil bereits vorsieht, wird in diesem Security Target darauf verzichtet, die Hierarchie der Komponenten sowie deren Abhängigkeiten zu wiederholen. Diese Informationen sind dem Schutzprofil [BSI-CC-PP-0098] zu entnehmen. Bei Sicherheitsanforderungen, die durch das Security Target hinzugefügt werden, sind die Hierarchie- und Abhängigkeitsinformationen aufgeführt.

6.1.1. Hinweise zur Notation

Die typographischen Auszeichnungen für die Operationen an den SFR sind in Tabelle 6.1 beschrieben. Die Anpassungen der Formatierungen gegenüber dem Schutzprofil [BSI-CC-PP-0097] dienen der Vereinheitlichung zwischen den Schutzprofilen [BSI-CC-PP-0097] und [BSI-CC-PP-0098]. ST-seitige Löschungen werden immer von einem Hinweis begleitet, wie die Löschung motiviert ist.

Quelle	Art der Anpassung	Typographische Eigenschaften
PP	Zuweisung (Assignment)	Zuweisungen sind unterstrichen gesetzt.
	Auswahl (Selection)	Auswahlen sind *kursiv und unterstrichen* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**fett und durchgestrichen**~~ gesetzt.
ST	Zuweisung (Assignment)	Zuweisungen sind in blauer Schrift gesetzt.
	Auswahl (Selection)	Auswahlen sind *in blauer Schrift und kursiv* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **in blauer Schrift und fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**in blauer Schrift, fett und durchgestrichen**~~ gesetzt.

Tabelle 6.1.: Typographische Konventionen

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

6.1.2.1. Hinweise zu Übernahmen aus dem Schutzprofil

Die Modellierungen des Schutzprofils [BSI-CC-PP-0098] gelten auch für dieses Security Target.

Die Architektur des TOE mit seinen Java Virtual Machines ist monolithischer als es die Definitionen der Subjekte im Schutzprofil suggerieren. Die dort definierten Subjekte wie S_AK, S_Signaturdienst, S_Chipkartendienst etc. sind grundsätzlich auch für die KoCoBox MED+ anwendbar. Jedoch manifestieren sie sich *nicht* in der Implementierung in Form von separaten Prozessen. Alle diese Subjekte

existieren in der JVM des Anwendungskonnektors. Innerhalb der JVM sind die Subjekte nicht physisch voneinander abgegrenzt. Das hat Implikationen auf die Sicherheitsanforderungen in den Familien FDP_ACC und FDP_ACF. Anforderungen wie „Nur der Chipkartendienst darf…“ werden nicht durch Kontrollmechanismen umgesetzt, sondern dadurch, dass aus der Implementierung heraus ersichtlich ist, dass keine Aufrufe stattfinden, die nicht in der Sicherheitsarchitektur vorgesehen sind.

6.2. Funktionale Sicherheitsanforderungen des Netzkonnektors

6.2.1. VPN Client

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

FTP_ITC.1.1/NK.VPN_TI	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/NK.VPN_TI	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/NK.VPN_TI	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

FTP_ITC.1.1/NK.VPN_SIS	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/NK.VPN_SIS	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/NK.VPN_SIS	Die in [BSI-CC-PP-0097, Abschnitt 6.2.1] und [BSI-CC-PP-0098, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

FDP_IFC.1/NK.PF
Subset information flow control

FDP_IFC.1.1/NK.PF	Die in [BSI-CC-PP-0097, Abschnitt 6.2.2] und [BSI-CC-PP-0098, Abschnitt 6.2.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_IFF.1/NK.PF
Simple security attributes

FDP_IFF.1.1/NK.PF	The TSF shall enforce the PF SFP 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 traffic),*

(5) **interface (inbound and outbound traffic).**

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

FDP_IFF.1.2/NK.PF

Die in [BSI-CC-PP-0097, Abschnitt 6.2.2] und [BSI-CC-PP-0098, Abschnitt 6.2.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

The usage of a VPN connection for security relevant data shall be enforced by using an appropriate set of policies of the network subsystem that demand data from the application connector to be routed into the VPN.

ST-Anwendungshinweis 1

Die Unterpunkte FDP_IFF.1.2/NK.PF(8), (11), (12) und (13) referenzieren den Betriebsmodus *MGM_LOGICAL_SEPARATION*, der in der Konnektor-Spezifikation entfallen ist [gemSpec_Kon]. Die logische Trennung ist nicht im TOE implementiert ist. Daher ist es nicht möglich, die Auswahl „logische Trennung“ zu aktivieren, somit gilt *MGM_LOGICAL_SEPARATION=Disabled*. Dieser Hinweis gilt auch für alle weiteren Vorkommen von *MGM_LOGICAL_SEPARATION*.

FDP_IFF.1.3/NK.PF

Die in [BSI-CC-PP-0097, Abschnitt 6.2.2] und [BSI-CC-PP-0098, Abschnitt 6.2.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_IFF.1.4/NK.PF

The TSF shall explicitly authorise an information flow based on the following rules: Stateful Packet Inspection, none[1].

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.

[1] Assignment: *rules, based on security attributes, that explicitly authorise information flow*

(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_BESTANDS-NETZE 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_ZEN-TRAL, NET_TI_GESICHERTE_FD, NET_TI_DE-ZENTRAL, ANLW_AKTIVE_BESTANDSNET-ZE, ANLW_LAN_ADDRESS_SEGMENT, AN-LW_LEKTR_INTRANET_ROUTES and AN-LW_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_LOGI-CAL_SEPARATION=Disabled and ANLW_INTER-NET_MODUS=KEINER).

(9) The TSF prevents inbound packets of the VPN channels from SIS with destination address in the inner header outside

1. ANLW_LAN_IP_ADDRESS or
2. ANLW_LEKTR_INTRANET_ROUTES if ANLW_WAN_ADAPTER_MODUS=DISABLED or
3. 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) All firewall rules defined in [gemSpec_Kon, Abschnitt 4.2.1.1.2] that call for traffic to be dropped.[2]

ST-Anwendungshinweis 2 — Die [gemSpec_Kon] gibt sämtliche Paketfilterregeln vor. Damit sind auch die erlaubten Protokolle durch [gemSpec_Kon, TIP1-A_4747] festgelegt: ICMP, IP in IP, UDP, TCP, ESP und IPComp. Da die Nutzung von IPComp insgesamt optional ist, lehnt der TOE das IPComp und das nur dann benötigte IP in IP Protokoll zusätzlich ab. Für das Protokoll ICMP gelten für die einzelnen ICMP-Typen die Bestimmungen aus [gemSpec_Kon] und [gemSpec_Net]

ST-Anwendungshinweis 3 — Das Fachmodul VSDM ist Teil des Anwendungskonnektors, somit gelten auch die Firewallregeln des Anwendungskonnektors.

Hintergrund: Das Fachmodul VSDM wird – anders als andere Fachmodule der Ausbaustufe OPB 2.1 – nicht nach Technischer Richtlinie, sondern nach Common Criteria zertifiziert, im selben Verfahren wie der Anwendungskonnektor. Das Schutzprofil [BSI-CC-PP-0098] formuliert die Sicherheitsanforderungen FDP_ACC.1/AK.VSDM und FDP_ACF.1/AK.VSDM an das Fachmodul. Dies verdeutlicht die architekturelle Einheit zwischen FM VSDM und Anwendungskonnektor.

FMT_MSA.3/NK.PF
Static attribute initialisation

FMT_MSA.3.1/NK.PF — Die in [BSI-CC-PP-0097, Abschnitt 6.2.2] und [BSI-CC-PP-0098, Abschnitt 6.2.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MSA.3.2/NK.PF — The TSF shall allow ~~the~~[3] nobody[4] to specify alternative initial values to override the default values when an object or information is created.

6.2.3. Netzdienste

FPT_STM.1/NK
Reliable time stamps

FPT_STM.1.1/NK — Die in [BSI-CC-PP-0097, Abschnitt 6.2.3] und [BSI-CC-PP-0098, Abschnitt 6.2.3] formulierten Sicherheitsanforderungen gelten ohne

[2] Assignment: *Additional rules, based on security attributes, that explicitly deny information flows*
[3] Deletion: *Editorielle Anpassung*
[4] Assignment: *the authorised identified roles*

Anpassung.

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 NTPv4 [RFC 5905] erreicht. Der EVG verwendet den verlässlichen Zeitstempel für sich selbst und bietet anderen Konnektorteilen eine Schnittstelle zur Nutzung des verlässlichen Zeitstempels an. Befindet sich der EVG im Online-Modus, muss er die Zeitsynchronisation mindestens bei Start-up, einmal innerhalb von 24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht nicht mehr als *3600 Sekunden*[5] von der Zeitinformation der darüber liegenden Stratum-Ebene ab.

ST-Anwendungshinweis 4 Der TOE benachrichtigt Benutzer auf seinem Display über kritische Betriebszustände. Das Display entspricht der „Signaleinrichtung“ des Konnektors, wie die Spezifikation sie fordert [gemSpec_Kon, TIP1-A_4843]. Der Netzkonnektor steuert das Display über die logische Schnittstelle LS.DISPLAY an. Das Schutzprofil fordert in Anwendungshinweis 87, dass die „Korrektheit der Kommunikation zwischen dem NK und anderen Konnektorteilen“ im Rahmen der Prüfung von FPT_STM.1/NK evaluiert wird. Aus diesem Grund werden Module der Subsysteme EventService und RMIBridge diesem SFR zugeordnet, auch wenn diese Subsysteme ursprünglich nicht im Zusammenhang mit der Zeitsynchronisation stehen.

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

FPT_TDC.1.1/NK.Zert Die in [BSI-CC-PP-0097, Abschnitt 6.2.3] und [BSI-CC-PP-0098, Abschnitt 6.2.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

The interpretation rules are defined in TUC_PKI_018 „Zertifikatsprüfung in der TI“ considering the verification mode „CRL“ [gemSpec_PKI, Abschnitt 8.3.1.1].

ST-Anwendungshinweis 5 Das Refinement des Schutzprofils zu FPT_TDC.1/NK.Zert verpflichtet den TOE zu prüfen, „dass […] sowohl TSL als auch CRL aktuell sind“. Dieses Refinement wird gemäß GS-A_4898 ergänzt durch den Verweis auf Tab_PKI_294, in der die Gültigkeit der TSL präzisiert wird.

[5] Selection: *nicht mehr als 330ms, [Zuweisung: andere Zeit]*

6.2.4. Stateful Packet Inspection

(This section intentionally left blank.)

6.2.5. Selbstschutz

FDP_RIP.1/NK
Subset residual information protection

FDP_RIP.1.1/NK	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: cryptographic keys (and session keys) used for the VPN or for TLS-connections, sensitive user data (zu schützende Daten der TI und der Bestandsnetze and zu schützende Nutzerdaten), no other objects[6].
Refinement:	Die sensitive Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. Reset, überschrieben werden. **These sensitive objects are overwritten with constant or pseudo-random values.**

FPT_TST.1/NK
TSF testing

FPT_TST.1.1/NK	The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorised user*[7] to demonstrate the correct operation of *stored TSF executable code*[8].
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3/NK	The TSF shall provide authorised users with the capability to verify the integrity of *stored TSF executable code*[9].
ST-Anwendungshinweis 6	The „stored TSF executable code“ comprises not only strictly the code, but all parts of the firmware such as XML schema files.

[6] Assignment: *list of objects*
[7] 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]*
[8] Selection: *[assignment: parts of TSF], the TSF*
[9] Selection: *[assignment: parts of TSF], the TSF*

FPT_EMS.1/NK
Emanation of TSF and User data

FPT_EMS.1.1/NK

The TOE shall not emit sensitive data (as listed below) – or information which can be used to recover such sensitive data – through network interfaces (LAN or WAN) in excess of limits that ensure that no leakage of this sensitive data occurs enabling access to

(1) session keys derived in course of the Diffie-Hellman Keyexchange Protocol,

(2) *key material used to verify the TOE's integrity during self tests*[10],

(3) *key material used to verify the integrity and authenticity of software updates*[11],

(4) *none*[12],

(5) *key material used for authentication of administrative users*[13],

(6) none[14] and

(7) data to be protected ("zu schützende Daten der TI und der Bestandsnetze")

(8) none[15].

FPT_EMS.1.2/NK

Die in [BSI-CC-PP-0097, Abschnitt 6.2.5] und [BSI-CC-PP-0098, Abschnitt 6.2.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FAU_GEN.1/NK.SecLog
Audit data generation

FAU_GEN.1.1/NK.SecLog

The TSF shall be able to generate an audit record of the following auditable events:

a) **Removed by refinement in [BSI-CC-PP-0098]**

b) All auditable events for the *not specified*[16] 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,

[10] Selection: *none, key material used to verify the TOE's integrity during self tests*
[11] Selection: *none, key material used to verify the integrity and authenticity of software updates*
[12] Selection: *none, key material used to decrypt encrypted software updates (if applicable)*
[13] Selection: *none, key material used for authentication of administrative users (if applicable)*
[14] Assignment: *list of other types of TSF data (may be empty)*
[15] Assignment: *list of types of user data (may be empty)*
[16] Selection: *choose one of: minimum, basic, detailed, not specified*

- IP addresses of the TOE are undefined or wrong,
- TOE could not perform system time synchronization within the last 30 days,
- during time synchronization, 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

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, and no other audit relevant information[17].

The TOE shall implement countermeasures against attacks attempting to flood the audit log in order to use the limited size of the audit log memory and the process of cyclically overwriting log memory to overwrite log entries that provide evidence of the attacker's activity.

ST-Anwendungshinweis 7

Die zu loggenden „auditable events" wurden mit der Zertifizierungsstelle und den Evaluatoren abgeglichen und die Konformität zu [gemSpec_Kon] wurde sichergestellt.

FAU_GEN.2/NK.SecLog
User identity association

FAU_GEN.2.1/NK.SecLog

Die in [BSI-CC-PP-0097, Abschnitt 6.2.5] und [BSI-CC-PP-0098, Abschnitt 6.2.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.2.6. Administration

FMT_SMR.1/NK
Security roles

FMT_SMR.1.1/NK

Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_SMR.1.2/NK

Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[17] Assignment: *other audit relevant information*

FMT_MTD.1/NK
Management of TSF data

FMT_MTD.1.1/NK

The TSF shall restrict the ability to *perform the operations in the „Operation" column of the following table on*[18] the real time clock, packet filtering rules and other TSF data named in the „Object" column of the following table[19] to the role Administrator.

Operation	Object
Modify	System time[20]
Create, Modify, Delete	Packet filtering rules
Perform	Self-tests
Perform	Software update
Perform	Activation and deactivation of VPN connections[21]

FIA_UID.1/NK.SMR
Timing of identification

FIA_UID.1.1/NK.SMR

Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_UID.1.2/NK.SMR

Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

Refinement:

Additionally, the TOE prevents the following TSF-mediated actions on behalf of the user before the user is identified:

- **All operations stated in FMT_MTD.1.1/NK.**

FTP_TRP.1/NK.Admin
Trusted path

FTP_TRP.1.1/NK.Admin

The TSF shall provide a communication path between itself and *local*[22] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*[23].

FTP_TRP.1.2/NK.Admin

The TSF shall permit *local users*[24] to initiate communication via the trusted path.

[18] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[19] Assignment: *list of other TSF data (may be empty)*
[20] Only available in offline mode, when there is no connection to the NTP servers.
[21] Please note that deactivation of a VPN connection also ensures that any network traffic which should be routed via the VPN is not possible at all.
[22] Selection: *remote, local*
[23] Selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*
[24] Selection: *the TSF, local users, remote users*

FTP_TRP.1.3/NK.Admin	Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 8	Der TOE setzt die Funktionalität für das Remote Management nicht um.

FMT_SMF.1/NK
Specification of Management Functions

FMT_SMF.1.1/NK	Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung. **The TOE shall be capable of performing all security management functions stated in FMT_MTD.1/NK.**

FMT_MSA.1/NK.PF
Management of security attributes

FMT_MSA.1.1/NK.PF	The TSF shall enforce the PF SFP to restrict the ability to *query, modify, delete*[25] the security attributes packet filtering rules to the roles „Administrator“, no other role[26]. The refinement from [BSI-CC-PP-0097] applies without modification.
ST-Anwendungshinweis 9	Die Firewallregeln sind fester Bestandteil des TOE und lassen sich somit nur durch ein Update des gesamten TOE aktualisieren.

FMT_MSA.4/NK
Security attribute value inheritance

FMT_MSA.4.1/NK	Die in [BSI-CC-PP-0097, Abschnitt 6.2.6] und [BSI-CC-PP-0098, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.2.7. Kryptographische Basisdienste

FCS_COP.1/NK.Hash
Cryptographic operation

FCS_COP.1.1/NK.Hash	The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-512[27] and cryptographic key sizes none that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4].

[25] Selection: *query, modify, delete, [assignment: other operations]*
[26] Assignment: *(may be empty): other authorised identified roles*
[27] Assignment: *list of SHA-2 Algorithms with more than 256 bit size*

FCS_COP.1/NK.HMAC
Cryptographic operation

FCS_COP.1.1/NK.HMAC	The TSF shall perform HMAC value generation and verification in accordance with a specified cryptographic algorithm HMAC with SHA-1, SHA-256[28] and cryptographic key sizes 160 and 256 bit[29] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4], RFC 2404 [RFC 2404], RFC 4868 [RFC 4868], RFC 7296 [RFC 7296].

FCS_COP.1/NK.Auth
Cryptographic operation

FCS_COP.1.1/NK.Auth	Die in [BSI-CC-PP-0097, Abschnitt 6.2.7] und [BSI-CC-PP-0098, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/NK.ESP
Cryptographic operation

FCS_COP.1.1/NK.ESP	Die in [BSI-CC-PP-0097, Abschnitt 6.2.7] und [BSI-CC-PP-0098, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/NK.IPsec
Cryptographic operation

FCS_COP.1.1/NK.IPsec	Die in [BSI-CC-PP-0097, Abschnitt 6.2.7] und [BSI-CC-PP-0098, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_CKM.1/NK
Cryptographic key generation

FCS_CKM.1.1/NK	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-HMAC-SHA1, PRF-HMAC-SHA256[30] and specified cryptographic key sizes 256 bit[31] that meet the following: specification [gemSpec_Krypt], TR-03116 [TR-03116-1].

[28] Assignment: *list of SHA-2 Algorithms with 256bit size or more*
[29] Assignment: *cryptographic key sizes*
[30] Assignment: *cryptographic key generation algorithm*
[31] Assignment: *cryptographic key sizes*

FCS_CKM.2/NK.IKE
Cryptographic key distribution

FCS_CKM.2.1/NK.IKE

Die in [BSI-CC-PP-0097, Abschnitt 6.2.7] und [BSI-CC-PP-0098, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

The following algorithms and preferences are supported for IKEv2 connections:

- **Diffie-Hellman Group 14**
- **DH exponent minimum length: 384 bits**
- **Forward secrecy: yes**
- **Encryption: AES-256-CBC**
- **Authentication: HMAC-SHA-1-96, HMAC-SHA-256-128**
- **PRF: PRF-HMAC-SHA1, PRF-HMAC-SHA-256**
- **Rekeying: IKE lifetime limited to 161 hours, IPsec SA lifetime limited to 23 hours**
- **Peer authentication: X.509 certificate with RSA 2048 bit keys**

FCS_CKM.4/NK
Cryptographic key destruction

FCS_CKM.4.1/NK

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method by overwriting with zeros[32] that meets the following: none[33].

6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

FTP_ITC.1.1/NK.TLS

Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1.2/NK.TLS

Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1.3/NK.TLS

The TSF shall initiate communication via the trusted channel for communication required by the Anwendungskonnektor, any connection specified in Table B.4.[34]

[32] Assignment: *cryptographic key destruction method*
[33] Assignment: *list of standards*
[34] Assignment: *list of other functions for which a trusted channel is required*

Refinement: Das Refinement im Schutzprofil [BSI-CC-PP-0098] gilt ohne Einschränkungen. Die umgesetzten Cipher Suiten aus dem Schutzprofil und der gematik Spezifikation [gemSpec_Krypt] werden in Tabelle B.1 auf Seite 147 wiederholt.

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

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

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

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

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

(4) importierte X.509 Zertifikate für Clientsysteme

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

(6) no other data types[35]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS.Zert The TSF shall use interpretation rules[36] when interpreting the TSF data from another trusted IT product.

The interpretation rules are defined in TUC_PKI_018 „Zertifikatsprüfung in der TI“ [gemSpec_PKI, Abschnitt 8.3.1.1]. The parameters for certificate validation are specified in GS-A_4663 [gemSpec_PKI, Abschnitt 8.4.1].[37]

Furthermore, GS-A_5215 [gemSpec_PKI, Abschnitt 9.1.2.2] defines rules for the interpretation of time stamps embedded in OCSP responses, which have to be taken into account when interpreting TSF data.[38]

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

FCS_CKM.1.1/NK.TLS Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

The following algorithms and preferences are supported for TLS key negotiation[39]

[35] Assignment: *additional list of data types*
[36] Assignment: *list of interpretation rules to be applied by the TSF*
[37] Refinement: *Präzisierung der Interpretationsregeln*
[38] Refinement: *Ergänzt gemäß Anforderungen aus GS-A_5215, vgl. Anhang D*
[39] Refinement: *Ergänzt gemäß Anforderungen aus GS-A_4384, vgl. Anhang D*

- **Diffie-Hellman Group 14 according to RFC 3526 [RFC 3526] for key establishment during TLS**
- **DH exponent shall have a minimum length of 384 bits**
- **Forward secrecy shall be provided**
- **Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves according to FIPS186-4 [FIPS PUB 186-2] as well as the brainpoolP256r1 and the brainpoolP384r1 curves according to RFC 5639 and RFC 7027 [RFC 5639; RFC 7027]**
- **Peer authentication (if required): X.509 certificate with RSA 2048 bit keys**

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

FCS_COP.1.1/NK.TLS.HMAC — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/NK.TLS.AES
Cryptographic operation

FCS_COP.1.1/NK.TLS.AES — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

FCS_COP.1.1/NK.TLS.Auth — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

FCS_CKM.1.1/NK.Zert — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA (using the random number generator specified by FCS_RNG.1/Hash_DRBG)[40] and specified cryptographic key sizes 2048 bit that meet the following: Standard OID 1.2.840.113549.1.1.11, RFC 4055 [RFC 4055], BSI TR-03116-1 [TR-03116-1].

The TSF shall

[40] Assignment: *Algorithm for cryptographic key generation of key pairs*

(1) **create a valid X.509 certificate [RFC 5280] with the generated RSA key pair and**

(2) **create a PKCS#12 file [RFC 7292][41] with the created certificate and the associated private key.**

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

FDP_ITC.2.1/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.2/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.3/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.4/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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) No further rule[42]

FDP_ETC.2/NK.TLS
Export of user data with security attributes

FDP_ETC.2.1/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ETC.2.2/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ETC.2.3/NK.TLS — Die in [BSI-CC-PP-0097, Abschnitt 6.2.8] und [BSI-CC-PP-0098, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[41] Refinement: *Die Quelle für den PKCS#12 Standard wurde gegenüber dem Schutzprofil aktualisiert.*
[42] Assignment: *additional importation control rules*

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) No further rule[43]

FMT_MOF.1/NK.TLS
Management of security functions behaviour

FMT_MOF.1.1/NK.TLS

The TSF shall restrict the ability to *determine the behaviour of* the functions Management of TLS-Connections required by the Anwendungskonnektor to Anwendungskonnektor.

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) No further rule[44]

[43] Assignment: *additional exportation control rules*
[44] Assignment: *additional rules*

If one or more of these rules are managed by the EVG itself, this shall also be interpreted as a fullfillment of this SFR.

ST-Anwendungshinweis 10 — Gemäß C_6968 und der daraus resultierenden Anforderung A_18464 darf TLS 1.1 nicht mehr verwendet werden. Der TOE setzt diese Anforderung um und unterstützt TLS 1.1 nicht mehr.

ST-Anwendungshinweis 11 — TLS wird vom Konnektor von JSSE implementiert. Jeder in Java implementierte Teil des TOE kann prinzipiell eine TLS-Verbindung eröffnen. Es gibt keine Kontrollinstanz, die die Einhaltung der oben genannten Konfigurationsparameter einer TLS-Verbindung erzwingt.

6.2.9. Zusätzliche Sicherheitsanforderungen

Dieser Abschnitt enthält Sicherheitsanforderungen, die zusätzlich zu denen des Schutzprofils definiert werden. Die Anforderungen an den Netzkonnektor werden hier um die in Kapitel 5.1 definierte Anforderung FCS_RNG.1/Hash_DRBG erweitert. Weiterhin werden Anforderungen definiert, deren Umsetzung notwendig für den sicheren Datenspeicher ist. Zwar ist der sichere Datenspeicher Teil des Gesamtkonnektors, dennoch werden bereits hier Aspekte berücksichtigt, die für die Speicherung des Sicherheitsprotokolls relevant sind.

FCS_RNG.1/Hash_DRBG
Zufallszahlenerzeugung

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RNG.1.1/Hash_DRBG — The TSF shall provide a *deterministic*[45] random number generator that implements: [46]

(1) If initialized with a random seed using PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 100 bits min-entropy.

(2) The RNG provides forward secrecy.

(3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2/Hash_DRBG — The TSF shall provide random numbers that meet: [47]

(1) The RNG gets initialized during every startup and after 2048 requests with a random seed of minimal 384 bits using a PTRNG of class PTG.2. The RNG generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability $w > 1 - 2^{(-16)}$.

[45] Selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*
[46] Assignment: *list of security capabilities*
[47] Assignment: *a defined quality metric*

(2) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

ST-Anwendungshinweis 12 — FCS_RNG.1/Hash_DRBG is implemented by Hash_DRBG with SHA-256 according to [NIST SP 800-90A, Sect. 10.1.1]. It is used for generation of ephemeral keys for Diffie-Hellman and nonces in the TLS protocol.

FCS_COP.1/Sign
Cryptographic Operation / Signature Verfication

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) not fulfilled in this ST as no keys have to be generated for signature verification. The key pair for signature generation/verification is stored on the gSMC-K and has been created during production.

FCS_CKM.4 Cryptographic key destruction is not fulfilled in this ST as only public keys are used for this operation.

FCS_COP.1.1/Sign — The TSF shall perform signature verification[48] in accordance with a specified cryptographic algorithm according to Tabelle 6.2[49] and cryptographic key sizes according to Tabelle 6.2[50] that meet the following: PKCS#1 [RFC 8017] and FIPS180-4 [FIPS PUB 180-4][51].

Algorithm	Key size (bits)	Purpose: Verification of…
RSASSA-PSS with SHA-256	2048	Signatures of TSL and CRL
RSASSA-PSS with SHA-512	2048	Firmware update signatures
RSASSA-PKCS1-1.5 with SHA-256	2048	Signatures of BNetzA-VL
RSASSA-PSS with SHA-256	4096	Signatures for X.509 certificates during the firmware update process

Tabelle 6.2.: Algorithms, Key sizes and Purposes of Signature Verification

[48] Assignment: *list of cryptographic operations*
[49] Assignment: *cryptographic algorithm*
[50] Assignment: *cryptographic key sizes*
[51] Assignment: *list of standards*

FCS_COP.1/Storage.AES
Cryptographic Operation / Secure Storage AES

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) not fulfilled by the TOE. The symmetric key is generated by the gSMC-K. FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/NK
FCS_COP.1.1/Storage.AES	The TSF shall perform symmetric encryption/decryption[52] in accordance with a specified cryptographic algorithm AES CBC with ESSIV[53] and cryptographic key sizes 256 bit[54] that meet the following: FIPS197 [FIPS PUB 197], SP800-38A [NIST SP 800-38A], and ESSIV [ESSIV][55].

6.3. Funktionale Sicherheitsanforderungen des Anwendungskonnektors

6.3.1. Klasse FCS: Kryptographische Unterstützung

6.3.1.1. Basisalgorithmen

Der Konnektor nutzt kryptographische Dienste der gSMC-K in der Einsatzumgebung. Das Schutzprofil COS [BSI-CC-PP-0082-2] 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

FCS_COP.1.1/AK.SHA	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_CKM.1/AK.AES
Cryptographic key generation / AES keys

FCS_CKM.1.1/AK.AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm randomly created according to FCS_RNG.1/Hash_DRBG[56] and specified cryptographic key

[52] Assignment: *list of cryptographic operations*
[53] Assignment: *cryptographic algorithm*
[54] Assignment: *cryptographic key sizes*
[55] Assignment: *list of standards*
[56] Assignment: *Algorithm for cryptographic key generation of AES keys*

sizes 128 bit and 256 bit that meet the following: NISTSP800-133 [NIST SP 800-133, Section 6.1][57].

FCS_CKM.4/AK
Cryptographic key destruction

FCS_CKM.4.1/AK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwrite with zeros[58] that meet the following none[59].

6.3.1.3. Signaturerzeugung und Signaturprüfung

FCS_COP.1/AK.SigVer.SSA
Cryptographic operation / Signature verification PKCS#1 SSA

FCS_COP.1.1/AK.SigVer.SSA	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.SigVer.PSS
Cryptographic operation / Signature verification PKCS#1 PSS

FCS_COP.1.1/AK.SigVer.PSS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.SigVer.ECDSA
Cryptographic operation / Signature verification ECDSA

FCS_COP.1.1/AK.SigVer.ECDSA	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.XML.Sign
Cryptographic operation / XML signature generation

FCS_COP.1.1/AK.XML.Sign	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.CMS.Sign
Cryptographic operation / CMS signature generation

FCS_COP.1.1/AK.CMS.Sign	Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[57] Assignment: *list of standards*
[58] Assignment: *cryptographic key destruction method*
[59] Assignment: *list of standards*

FCS_COP.1/AK.PDF.Sign
Cryptographic operation / PDF signature generation

FCS_COP.1.1/AK.PDF.Sign — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.XML.SigPr
Cryptographic operation / XML Signature verification

FCS_COP.1.1/AK.XML.SigPr — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.CMS.SigPr
Cryptographic operation / CMS Signature verification

FCS_COP.1.1/AK.CMS.SigPr — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.PDF.SigPr
Cryptographic operation / PDF Signature verification

FCS_COP.1.1/AK.PDF.SigPr — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.PKCS.SigPr
Cryptographic operation / PKCS Signature verification

FCS_COP.1.1/AK.PKCS.SigPr — The TSF shall perform verify signed binary data with a specified cryptographic algorithm

(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

and cryptographic key sizes 1976 bit to 4096 bit[60] that meet the following: RFC 8017 [RFC 8017] and FIPS PUB 180-4 [FIPS PUB 180-4]

6.3.1.4. Ver- und Entschlüsselung von Dokumenten

FCS_COP.1/AK.AES
Cryptographic operation / AES encryption and decryption

FCS_COP.1.1/AK.AES — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[60] Assignment: *cryptographic key sizes*

FCS_COP.1/AK.XML.Ver
Cryptographic operation / XML encryption

FCS_COP.1.1/AK.XML.Ver — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.XML.Ent
Cryptographic operation / XML decryption

FCS_COP.1.1/AK.XML.Ent — The TSF shall perform decryption of XML documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm *RSAOAEP*[61] and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST-SP-800-38D [NIST SP 800-38D], FIPS 197 [FIPS PUB 197] and XMLEnc [XMLEnc]

FCS_COP.1/AK.MIME.Ver
Cryptographic operation / MIME encryption

FCS_COP.1.1/AK.MIME.Ver — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.MIME.Ent
Cryptographic operation / MIME decryption

FCS_COP.1.1/AK.MIME.Ent — The TSF shall perform decryption of MIME documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm *RSAOAEP*[62] and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST-SP-800-38D [NIST SP 800-38D], PKCS#1 [RFC 8017], FIPS 197 [FIPS PUB 197] and RFC 5751 [RFC 5751]

FCS_COP.1/AK.CMS.Ver
Cryptographic operation / CMS encryption

FCS_COP.1.1/AK.CMS.Ver — Die in [BSI-CC-PP-0098, Abschnitt 6.3.1.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/AK.CMS.Ent
Cryptographic operation / CMS decryption

FCS_COP.1.1/AK.CMS.Ent — The TSF shall perform decryption of documents in accordance with a specified cryptographic algorithm *RSAOAEP*[63] and AES-GCM with authentication tag length of 128 bit and cryptographic key

[61] Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP*
[62] Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP*
[63] Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP*

sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST-SP-800-38D [NIST SP 800-38D], PKCS#1 [RFC 8017], FIPS 197 [FIPS PUB 197] and CMS [RFC 5652]

6.3.2. Klasse FIA: Identifikation und Autorisierung

FIA_SOS.1/AK.Passwörter

Verification of secrets / Passwords

FIA_SOS.1.1/AK.Passwörter

The TSF shall provide a mechanism to verify that administrator passwords meet the following criteria:[64]

- A password consists of the following character classes: uppercase letters, lowercase letters, special characters and numbers.
- A password must contain at least one character of three of the aforementioned character classes.
- A password must consist of at least 8 characters.
- A password must not contain the user's user ID, neither forward nor backward, in neither lowercase nor uppercase characters.
- Upon password change, the TSF must consider previously entered passwords. At least the three most recently used passwords in the user's password history must be rejected when changing the password.

ST-Anwendungshinweis 13

Die Zuweisungen in diesem SFR setzen die Anforderungen aus TIP1-A_4808 um.

FIA_SOS.1/AK.CS.Passwörter

Verification of secrets / Passwords for client systems

FIA_SOS.1.1/AK.CS.Passwörter

The TSF shall provide a mechanism to verify that passwords for client systems meet the following criteria:[65]

- A password consists of the following character classes: uppercase letters, lowercase letters, numbers, space, dot, hyphen and underscore.

ST-Anwendungshinweis 14

Das verfügbare Alphabet umfasst 66 Zeichen. Bei einer Länge von 17 Zeichen ergibt sich eine Entropie von 102 Bit. Der Hersteller sieht dies als ausreichend sicher an. Um die Interoperabilität mit Clientsystemen zu wahren, werden auch Passwörter mit mindestens 6 Zeichen Länge akzeptiert. Wenn das Passwort kürzer als 17 Zeichen und länger als 6 Zeichen ist, erscheint eine Warnung. Darüber hinaus erhält der Dialog die Möglichkeit zur Generierung eines sicheren Passworts mit mindestens 17 Zeichen. Als Quelle für dieses Passwort wird der gSMC-K-basierte Zufallsgenerator herangezogen.

[64] Assignment: *a defined quality metric*
[65] Assignment: *a defined quality metric*

FIA_SOS.2/AK.PairG
Generation of pairing secrets

FIA_SOS.2.1/AK.PairG — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_SOS.2.2/AK.PairG — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_UID.1/AK
Timing of identification

FIA_UID.1.1/AK — The TSF shall allow

(1) Self test according to FPT_TST.1/AK.Out-Of-Band,

(2) (no further action).[66]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/AK — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_UAU.1/AK
Timing of authentication

FIA_UAU.1.1/AK — The TSF shall allow

(1) Identification of an user of the administrative interface, an user of the a Clientsytem, a smart card and a eHealth cardterminal,

(2) Signature verification according to **FDP_ACF.1/AK.SigPr,**

(3) Encryption according to FDP_ACF.1/AK.Enc,

(4) Handover of a card handle of an identified smart card,

(5) no further action.[67]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/AK — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_UAU.5/AK
Multiple authentication mechanisms

FIA_UAU.5.1/AK — The TSF shall provide

(1) *password based authentication mechanism*[68] for administrator users,

[66] Assignment: *list of TSF-mediated actions*
[67] Assignment: *list of TSF mediated actions*
[68] Selection: *password based authentication mechanism, [another authentication mechanism]*

(2) TLS authentication with a pairing secret for eHKT [gemSpec_Kon], 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,

(5) **password based and certificate based authentication mechanisms for client systems**[69]

to support user authentication.

ST-Anwendungshinweis 15 — Unterpunkt (2) muss interpretiert werden: Die Formulierung „TLS authentication with a pairing secret“ legt nahe, dass das Pairing-Geheimnis für die gegenseitige Authentisierung im Rahmen des TLS-Handshakes verwendet werden soll.

TLS-Handshake und Verwendung des Pairing-Geheimnisses geschehen jedoch auf unterschiedlichen Ebenen. Zuerst findet ein protokollkonformer TLS-Handshake statt, um eine beidseitig authentisierte TLS-Verbindung zu initiieren. Für diesen Handshake spielt das Pairing-Geheimnis keine Rolle. Die SICCT-Authentisierung findet auf der Ebene des Anwendungsprotokolls statt und ist – aus Sicht des Protokollstapels – oberhalb des TLS-Protokolls.

ST-Anwendungshinweis 16 — Unterpunkt (5) bezieht sich auf die Anforderung TIP1-A_4516 in der Konnektor-Spezifikation, in der die Authentisierungsverfahren für Clientsystem beschrieben sind.

FIA_UAU.5.2/AK — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_API.1/AK
Authentication Proof of Identity

FIA_API.1.1/AK — Die in [BSI-CC-PP-0098, Abschnitt 6.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_API.1/AK.TLS
Authentication Proof of Identity / TLS

FIA_API.1.1/TLS — The TSF shall provide a TLS authentication mechanism using AK.AUT certificate[70] to prove the identity of the TOE[71].

ST-Anwendungshinweis 17 — Eigenes SFR hinzugefügt auf Basis der Anforderung GS-A_4384.

[69] Refinement: *Ergänzt gemäß Anforderungen aus TIP1-A_4516, vgl. Anhang D*
[70] Assignment: *authentication mechanism*
[71] Assignment: *identity or role*

6.3.3. Klasse FDP: Schutz der Benutzerdaten

Die in den FDP_ACC/FDP_ACF-Anforderungen verwendeten Dienste-Bezeichnungen sind nur eine Orientierung und keine verbindlichen Dienste. Diese SFR stellen keine Anforderungen an die Architektur des TOE. Die Subjekte aus den SFR sind beispielhaft zu verstehen und dienen zum besseren Verständnis der funktionalen Anforderungen. Sie können je nach Umsetzung angepasst (z. B. zusammengefasst oder interpretiert) werden. Diese Annahme gilt für alle im Folgenden beschriebenen SFR.

Durch die Modellierung der Subjekte und Objekte im Schutzprofil besteht zumindest die Interpretationsmöglichkeit, dass das Schutzprofil Architekturblöcke definiert. Die Architektur des vorliegenden TOE fasst im Schutzprofil definierte Subjekte und Objekte zusammen, sodass in der vorliegenden Implementierung die geforderten Abgrenzungen zwischen den Diensten per Konvention durchgesetzt werden.

6.3.3.1. Zugriffskontrolldienst

FDP_ACC.1/AK.Infomod
Subset access control / Informationsmodell

FDP_ACC.1.1/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.Infomod
Security attribute based access control / Informationsmodell

FDP_ACF.1.1/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.2/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.3/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.4/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MSA.1/AK.Infomod
Management of security attributes / Informationsmodell

FMT_MSA.1.1/AK.Infomod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MSA.3/AK.Infomod
Static attribute initialization / Informationsmodell

FMT_MSA.3.1/AK.Infomod	The TSF shall enforce the Infomodell-SFP to provide *no*[72] default values for security attributes that are used to enforce the SFP.

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

FMT_MSA.3.2/AK.Infomod — The TSF shall allow the *no role*[73] to specify alternative initial values to override the default values when an object or information is created.

ST-Anwendungshinweis 18 — Es gibt keine vom Administrator überschreibbaren Konfigurationswerte. Folglich gibt es auch keine alternativen Anfangswerte. Die Anforderung ist implizit erfüllt.

6.3.3.2. Kartenterminaldienst

FDP_ACC.1/AK.eHKT

Subset access control / Kartenterminaldienst

FDP_ACC.1.1/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.eHKT

Security attribute based access control / Kartenterminaldienst

FDP_ACF.1.1/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.2/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.3/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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) The subject S_Kartenterminaldienst must not send SICCT or EHEALTH-Commands to a card terminal for which *CT.CONNECTED=Nein* is set, with the exception of the commands listed in TAB_KON_785 [gemSpec_Kon].[74]

ST-Anwendungshinweis 19 — Die zusätzliche Regel in FDP_ACF.1.4/AK.eHKT(2) greift die Anforderung TIP1-A_6478 der Konnektor-Spezifikation auf.

[73] Selection: *S_Administrator, no role*
[74] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*

FDP_UCT.1/AK.TLS
Basic data exchange confidentiality

FDP_UCT.1.1/AK.TLS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_UIT.1/AK.TLS
Basic data exchange integrity

FDP_UIT.1.1/AK.TLS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_UIT.1.2/AK.TLS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MTD.1/AK.eHKT_Abf
Management of TSF data / eHealth-Kartenterminal Abfrage

FMT_MTD.1.1/AK.eHKT_Abf	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MTD.1/AK.eHKT_Mod
Management of TSF data / eHealth-Kartenterminal Modifikation

FMT_MTD.1.1/AK.eHKT_Mod	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.2] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.3.3.3. Chipkartendienst

FDP_ACC.1/AK.KD
Subset access control / Chipkartendienst

FDP_ACC.1.1/AK.KD	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.KD
Security attribute based access control / Chipkartendienst

FDP_ACF.1.1/AK.KD	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.2/AK.KD	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 20	Die Anforderung aus FDP_ACF.1.2/AK.KD(1) muss in Bezug auf das Caching der Daten präzisiert werden: Alle zwischengespeicherten Daten, die über das Kartenhandle mit der Karte assoziiert werden, werden – sofern die Karte noch nicht entfernt wurde – nach 24 Stunden gelöscht und neu erzeugt. Für *eGK, HBAx* gilt zusätzlich, dass die existierenden Kartensitzungen gelöscht werden (vgl. auch TIP1-A_4558, bzw. TIP1-A_6031.)

FDP_ACF.1.3/AK.KD — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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/AK.KD 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) No further rule.[75]

FDP_ACC.1/AK.PIN
Subset access control / PIN

FDP_ACC.1.1/AK.PIN — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.PIN
Security attribute based access control / PIN

FDP_ACF.1.1/AK.PIN — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.2/AK.PIN — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.3/AK.PIN — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[76].

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 DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, VERIFY, RESET RETRY COUNTER, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT oder CHANGE REFERENCE DATA absetzen.

[75] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[76] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*

(2) Kein Subjekt außer S_Fachmodul darf eine PIN-Eingabe zur PIN-Prüfung für eine eGK bei S_Chipkartendienst anfordern.

(3) no further rule[77].

6.3.3.4. Signaturdienst

FIA_SOS.2/AK.Jobnummer
TSF generation of secrets / Jobnummer

FIA_SOS.2.1/AK.Jobnummer — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FIA_SOS.2.2/AK.Jobnummer — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACC.1/AK.Sgen
Subset access control / Signaturerstellung

FDP_ACC.1.1/AK.Sgen — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.Sgen
Security attribute based access control / Signaturerstellung

FDP_ACF.1.1/AK.Sgen — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.2/AK.Sgen — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.3/AK.Sgen — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[78].

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.

[77] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[78] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*

(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) keine weiteren Einschränkungen[79]

zugreifen.

(5) no further rule[80].

FDP_ACC.1/AK.SigPr

Subset access control / Signature verification

FDP_ACC.1.1/AK.SigPr	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.SigPr

Security attribute based access control / Signature verification

FDP_ACF.1.1/AK.SigPr	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.2/AK.SigPr	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.3/AK.SigPr	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[81].
FDP_ACF.1.4/AK.SigPr	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: no further rule[82].

[79] Assignment: *weitere Signaturschlüssel externer Signaturchipkarten*
[80] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[81] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[82] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*

FDP_DAU.2/AK.QES

Data Authentication with Identity of Guarantor / Qualifizierte elektronische Signatur

FDP_DAU.2.1/AK.QES

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of data to be signed **durch qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der qualifizierten Signaturerstellungseinheit (QSEE) zur Erzeugung der digitalen Signatur. Es sind die Dokumentenformate zu signierender Daten**

(1) **Text-Dateien (UTF-8 [Unicode] oder ISO-8859-15 [ISO 8859-15]),**

(2) **TIFF-Dateien [TIFF],**

(3) **Adobe Portable Document Format (PDF/A) [ISO 19005; ISO 19005-1],**

(4) **XML-Dateien [XML; XSLT]**

und die Formate signierter Daten

(1) **PAdES [PAdES; PAdES-BL] für PDF/A-Dokumente,**

(2) **CAdES [CAdES; CAdES-BL] für XML, PDF/A, Text und TIFF Dokumente,**

(3) **XAdES [XAdES; XAdES-BL] für XML-Dokumente**

mit den Signaturvarianten

(1) **enveloped signature,**

(2) **enveloping signature,**

(3) **detached signature**[83]

zu unterstützen.

ST-Anwendungshinweis 21

Anwendungshinweis 160 des Schutzprofils eröffnet dem Hersteller die Möglichkeit, auch *detached signatures* zu verwenden, falls ein Fachmodul dies erfordert. Das Fachmodul NFDM (OPB 2.1) benötigt eine solche Signatur. Der TOE stellt diese bereit. Die Möglichkeit der detached signature gilt ausschließlich im Kontext von XML-Signaturen.

ST-Anwendungshinweis 22

Die Konnektorspezifikation schränkt die Kombinationsmöglichkeiten von Dokumentformaten, Signaturformaten und Signaturvarianten in TAB_KON_778 deutlich ein. Der TOE folgt der Konnektorspezifikation und setzt die Kombinationsmöglichkeiten entsprechend TAB_KON_778 um.

[83] Refinement: *vgl. ST-Anwendungshinweis 21*

FDP_DAU.2.2/AK.QES

The TSF shall provide S_Benutzern with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence **durch qualifizierte elektronische Signatur in den in FDP_DAU.2.1/AK.QES genannten Formaten sowie PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [RFC 8017]**

Dies sind im einzelnen:

(1) **ob die signierten Daten unverändert sind, d. h. das Ergebnis der Korrektheitsprüfung der digitalen Signatur über die signierten Daten,**

(2) **der der Signatur zuzuordnende Signaturschlüssel-Inhaber,**

(3) **die Inhalte des Zertifikates, auf dem die Signatur beruht,**

(4) **das Ergebnis der Nachprüfung der Zertifikate nach dem Kettenmodell, d. h. die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,**

   a. **der angenommene Signaturerstellungszeitpunkt, wobei gegen folgende Zeitpunkte zu prüfen ist, sofern die Voraussetzungen durch die zu prüfenden Daten erfüllt sind:**

      i. **vom Benutzer definierter Zeitpunkt, sonst**

      ii. **in der Signatur eingebetteter Zeitpunkt, sonst**

      iii. ***none*[84]**,

      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 Zertifikats mit Ausnahme des Wurzelzertifikats,**

   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**

   a. **die kryptographische Prüfung der digitalen Signatur mit dem dazugehörigen öffentlichen Schlüssel deren Korrektheit bestätigt hat oder nicht,**

[84] Selection: *none, qualifizierter Zeitstempel über die Signatur*

b. **die für 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) keine weiteren Nachweise[85].

FDP_DAU.2/AK.Sig
Data Authentication with Identity of Guarantor / NonQES

FDP_DAU.2.1/AK.Sig	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 23	Die Konnektorspezifikation schränkt die Kombinationsmöglichkeiten von Dokumentformaten, Signaturformaten und Signaturvarianten in TAB_KON_778 deutlich ein. Der TOE folgt der Konnektorspezifikation und setzt die Kombinationsmöglichkeiten entsprechend TAB_KON_778 um.
FDP_DAU.2.2/AK.Sig	The TSF shall provide S_Benutzern with the ability to verify evidence of the validity of the indicated information **~~and the identity of the user that generated the evidence~~ durch nicht-qualifizierte elektronische Signatur in den in FDP_DAU.2.1/AK.Sig genannten Formaten sowie PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [RFC 8017] gemäß gültiger Signaturrichtlinie bereitstellen. 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,** (6) keine weiteren Nachweise[86].

[85] Assignment: *andere Form von Nachweisen*
[86] Assignment: *andere Form von Nachweisen*

FDP_DAU.2/AK.Cert
Data Authentication with Identity of Guarantor / Überprüfung von Zertifikaten

FDP_DAU.2.1/AK.Cert — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_DAU.2.2/AK.Cert — The TSF shall provide S_Benutzern with the ability to verify evidence of the validity of the indicated **Zertifikatsprüfung, einschließlich Zertifikatsinhalt ~~information~~** and the identity of the user that generated the evidence. **Dies sind im einzelnen:**

(1) **der Inhalt des Zertifikats, auf dem die Signatur beruht,**

(2) **die zugehörigen Attribut-Zertifikate,**

(3) **der der Signatur zuzuordnende Signaturschlüssel-Inhaber,**

(4) **die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,**

(5) **das Ergebnis der Korrektheitsprüfung der Signatur,**

(6) **die Daten, auf die sich die Signatur bezieht,**

(7) **ob die signierten Daten unverändert sind,**

(8) **die Anforderung von OCSP-Anfragen und die Auswertung von OSCP-Antworten,**

(9) **die Anforderung von CRL-Anfragen und die Auswertung von CRL,**

(10) keine weiteren Nachweise.[87]

FDP_ITC.2/AK.Sig
Import of user data / Signaturdienst

FDP_ITC.2.1/AK.Sig — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.2/AK.Sig — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.3/AK.Sig — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.4/AK.Sig — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ITC.2.5/AK.Sig — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[87] Assignment: *andere Form von Nachweisen*

FMT_MSA.3/AK.Sig
Static attribute initialization / Signatur

FMT_MSA.3.1/AK.Sig	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FMT_MSA.3.2/AK.Sig	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 24	Es gibt keine vom Administrator überschreibbaren Konfigurationswerte. Folglich gibt es auch keine alternativen Anfangswerte. Die Anforderung ist implizit erfüllt.

FDP_SDI.2/AK
Stored data integrity monitoring and action

FDP_SDI.2.1/AK	The TSF shall monitor ~~**user data**~~ **zu signierende Daten** stored in containers controlled by the TSF for Veränderung on all objects, based on the following attributes: SHA-256 hash of the data[88].
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) keine weiteren Aktionen ausführen.[89]

FMT_MSA.1/AK.User
Management of security attributes / Clientsystem-Benutzer

FMT_MSA.1.1/AK.User	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 25	Da der Begriff Signaturrichtlinie im PP abstrakt alle Input-Parameter einer Signaturerstellung oder -prüfung umfasst, wird FMT_MSA.1.1/AK.User(2) dahingehend interpretiert, dass die Auswahl von Parametern durch den Benutzer des Clientsystems durchgeführt wird, vgl. auch die Beschreibung zu SF.SignatureService in Abschnitt 7.2.7.

FTP_ITC.1/AK.QSEE
Inter-TSF trusted channel / QSEE

FTP_ITC.1.1/AK.QSEE	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[88] Assignment: *user data attributes*
[89] Assignment: *weitere auszuführende Aktion*

FTP_ITC.1.2/AK.QSEE	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/AK.QSEE	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 26	FTP_ITC.1.3/AK.QSEE bezieht sich auf die Stapelsignatur. Für eine Einfachsignatur ist die Nutzung von Secure Messaging nicht erforderlich (vgl. [gemSpec_Kon, TIP1-A_4670].

FTA_TAB.1/AK.Jobnummer
TOE access warning / Jobnummer

FTA_TAB.1.1/AK.Jobnummer	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTA_TAB.1/AK.SP
TOE access warning / Fehler des Signaturprozesses

FTA_TAB.1.1/AK.SP	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 27	Die Kommunikation zwischen TOE und S_Benutzer_Clientsystem erfolgt über SOAP-Nachrichten und deren Interpretation durch die Benutzerschnittstelle des Clientsystemems. Der TOE hat selbst keine visuelle Benutzerschnittstelle zum Subjekt S_Benutzer_Clientsystem, über die die Warnung ausgegeben werden kann. Folglich wird das Refinement so interpretiert, dass die geforderte *advisory warning message* über die Antwort zum SOAP-Request übermittelt wird.

6.3.3.5. Software-Update

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

FDP_ACC.1.1/AK.Update	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

FDP_ACF.1.1/AK.Update	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ACF.1.2/AK.Update	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1.3/AK.Update — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[90].

FDP_ACF.1.4/AK.Update — The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) S_AK und S_NK dürfen Update-Pakete nicht automatisch anwenden, wenn die automatische Aktualisierung der Firmware durch S_Administrator deaktiviert wurde.

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

(3) **Wenn ein Update-Paket mit *FWPriority=Kritisch* vorhanden ist, dessen Deadline abgelaufen ist, so darf die TSF keine Kommunikation mit der TI Plattform herstellen und muss bestehende Verbindungen zur TI Plattform abbauen.**[91]

ST-Anwendungshinweis 28 — Der TOE unterstützt die automatische Anwendung von Update-Paketen nicht.

ST-Anwendungshinweis 29 — TIP1-A_6025 wird umgesetzt durch Unterpunkt FDP_ACF.1.1/AK.Update(3).

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

FDP_UIT.1.1/AK.Update — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_UIT.1.2/AK.Update — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.3.3.6. Verschlüsselungsdienst

FDP_ACC.1/AK.Enc
Subset access control / Verschlüsselung

FDP_ACC.1.1/AK.Enc — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[90] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[91] Refinement: *Ergänzt gemäß Anforderungen aus TIP1-A_6025, vgl. Anhang D*

FDP_ACF.1/AK.Enc

Security attribute based access control / Verschlüsselung

FDP_ACF.1.1/AK.Enc

Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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.

Der Verschlüsselungsdienst darf Requests zur Verschlüsselung nur akzeptieren, wenn sie konform zur gematik Spezifikation sind, vgl. [gemSpec_Kon, TAB_KON_739, TUC_KON_070].[92]

(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

1. die identifizierte Verschlüsselungsrichtlinie für die übergebenen zu verschlüsselnden Daten zulässig ist,
2. die identifizierte Verschlüsselungsrichtlinie die automatische Verschlüsselung erlaubt,
3. 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.

Der Verschlüsselungsdienst darf Requests zur Entschlüsselung nur akzeptieren, wenn sie konform zur Gematik Spezifikation sind, vgl. [gemSpec_Kon, TAB_KON_140 TUC_KON_071].[93]

(5) Das Subjekt S_Verschlüsselungsdienst darf nur dann die verschlüsselten Daten automatisch für die identifizierten vorgesehenen Empfänger entschlüsseln und die entschlüsselten Daten an die Subjekt S_AK zurückgeben, wenn

[92] Refinement: *vgl. ST-Anwendungshinweis 30*
[93] Refinement: *vgl. ST-Anwendungshinweis 30*

1. die identifizierte Verschlüsselungsrichtlinie für die übergebenen zu verschlüsselten Daten zulässig ist,
2. die identifizierte Verschlüsselungsrichtlinie die automatische Entschlüsselung erlaubt,
3. der Sicherheitsstatus der Chipkarte des identifizierten vorgesehenen Empfängers das Entschlüsseln des Dateischlüssels erlaubt.

FDP_ACF.1.3/AK.Enc — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[94].

FDP_ACF.1.4/AK.Enc — The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[95].

ST-Anwendungshinweis 30 — Der Begriff „Verschlüsselungsrichtlinie“ muss interpretiert werden. Im PP wird der Begriff im Glossar definiert. Er umfasst im wesentlichen das Verschlüsselungsformat (CMS oder XMLSec), den Herausgeber der Verschlüsselungsrichtlinie und – im Fall von XMLSec – das XML-Schema und die Information, ob der Schlüssel im Dokument steht. Die gematik Spezifikation verwendet den Begriff der Verschlüsselungsrichtlinie nicht, definiert aber dei Aufrufparameter für die Operationen *EncryptDocument* und *DecryptDocument*. Die gematik Spezifikation ist damit deutlich präziser als das Schutzprofil. Daher gilt für dieses Security Target die folgende Interpretation.

Die Forderung nach einer *zulässigen Verschlüsselungsrichtlinie* wird so interpretiert, dass die gegebene Kombination von Aufrufparametern im Rahmen des spezifizierten Regelwerkes als gültig bewertet wird. Für den TOE werden die Vorgaben der Konnektor Spezifikation als Regelwerk angenommen. Die Eingangsdaten der TUCs TUC_KON_070 und TUC_KON_071 liefern sehr präzise Vorgaben für die Parameter. Die Interpretation gilt nicht nur hier, sondern auch für alle weiteren Vorkommen von „Verschlüsselungsrichtlinie“ in diesem Security Target.

Weiterhin legt die Formulierung „Identität der Verschlüsselungsrichtlinie“ nahe, dass es eine Sammlung benannter (und damit referenzierbarer) Verschlüsselungsrichtlinien gibt. Das ist ein historisches Relikt, das sich aus der gematik Spezifikation nicht herleiten lässt und im vorliegenden TOE nicht umgesetzt ist.

FDP_ITC.2/AK.Enc
Import of user data with security attributes / Verschlüsselungsdienst

FDP_ITC.2.1/AK.Enc — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[94] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[95] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*

FDP_ITC.2.2/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ITC.2.3/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ITC.2.4/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ITC.2.5/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 31	Die Anforderung FDP_ITC.2.5/AK.Enc(2) wird so interpretiert, dass die Prüfung der Gültigkeit der Verschlüsselungszertifikate vor deren Verwendung zur Verschlüsselung eines Dokuments erfolgen muss.

FDP_ETC.2/AK.Enc

Export of user data with security attributes / Verschlüsselungsdienst

FDP_ETC.2.1/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ETC.2.2/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FDP_ETC.2.3/AK.Enc	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
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) No further rules[96].
ST-Anwendungshinweis 32	Die Anforderung FDP_ETC.2.4/AK.Enc(2) wird so interpretiert, dass die entschlüsselten Daten ausschließlich an den vorgesehenen Empfänger ausgeliefert werden. Die Identität des Empfängers manifestiert sich nicht in der Datenstruktur der Ausgabe der Operation. Die Spezifikation der gematik gibt ein solches Identifizierungsmerkmal nicht

[96] Assignment: *additional exportation control rules*

her[97]. In der vorliegenden Implementierung werden die entschlüsselten Daten in genau der HTTP-Response übertragen, die zu dem Request gehört, über den die zu entschlüsselnden Daten in den TOE importiert wurden. Damit ist die eindeutige Zuordnung des Empfängers gewährleistet.

6.3.3.7. TLS-Kanäle

FDP_ACC.1/AK.TLS
Subset access control / TLS-Kanäle

FDP_ACC.1.1/AK.TLS — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

ST-Anwendungshinweis 33 — Der Begriff „TLSConnectionIdentifier“ wird hier ausschließlich als Maßnahme zur Unterscheidung verschiedener TLS-Verbindungen betrachtet. Diese Maßnahme wird nicht notwendigerweise durch ein Sicherheitsattribut umgesetzt. Im TOE wird die Separation der TLS-Verbindungen durch Socket-Abstracktionen und die darauf basierenden Objektreferenzen umgesetzt, die vom Framework JSSE implementiert werden. Die Objektreferenzen sind als `private` gekennzeichnet oder lokale Variablen, sind also nur innerhalb des aktuellen Threads erreichbar.

Weiterhin setzt der TOE kein Subjekt S_TLS_Dienst um. Die Gematik-Spezifikation [gemSpec_Kon] sieht keinen zentralen Dienst für das Erstellen, die Verwaltung oder den Abbau von TLS-Verbindungen vor.

FDP_ACF.1/AK.TLS
Security attribute based access control / TLS-Kanäle

FDP_ACF.1.1/AK.TLS — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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

(1) Das S_AK baut auf Anforderung des Fachmoduls die TLS-Verbindung zum Fachdienst (TLS Server) auf und gibt den TLSConnectionIdentifier an den Aufrufenden zurück.

(2) Auf Anforderung des Clientsystems (als TLS Client) baut das S_AK (als TLS-Server) einen TLS-Kanal zum Clientsystem auf.

[97] TAB_KON_140 definiert als „Ausgangsdaten“ des TUC_KON_071 „Daten hybrid entschlüsseln“ lediglich: „plainDocument (Unverschlüsseltes Dokument. Bei XML-Dokumenten: Das EncryptedData-Element ist durch das entschlüsselte ersetzt.)“ Die Ausgangsdaten des TUC sehen die Übergabe der Identität des Empfängers nicht vor.

(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 eine 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 der 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) Keine weiteren Regeln[98]

FDP_ACF.1.3/AK.TLS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[99].

[98] Assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*

[99] 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) no further rules[100]

FMT_MSA.1/AK.TLS
Management of security attributes / TLS-Kanäle

FMT_MSA.1.1/AK.TLS

The TSF shall enforce the AK-TLS-SFP to restrict the ability to change_default, query, modify, delete, none[101] the security attributes Authentisierungsmechanismus[102] to S_Administrator.

Änderungen der Konfiguration müssen unmittelbar durchgesetzt werden.

ST-Anwendungshinweis 34

Die Konnektor-Spezifikation definiert in TAB_KON_852 zu TIP1-A_5009 die Zugriffsregeln, die sich aus den Kombinationen der Konfigurationswerte ergeben. Das Assignment „Authentisierungsmechanismus“ schließt diese Konfigurationswerte ein.

FMT_MSA.3/AK.TLS
Static attribute initialization / TLS-Kanäle

FMT_MSA.3.1/AK.TLS

The TSF shall enforce the AK-TLS-SFP to provide *unmodifiable*[103] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/AK.TLS

Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[100] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[101] Assignment: *other operations*
[102] Assignment: ***Authentisierungsmechanismus**, list of **additional** security attributes*
[103] Selection: *choose one of: restrictive, permissive, [assignment: other property]*

ST-Anwendungshinweis 35	Es gibt keine vom Administrator konfigurierbaren Anfangswerte für TLS-Verbindungen. Alle Konfigurationswerte für TLS Verbindungen sind durch [gemSpec_Krypt] vorgegeben und hart verdrahtet, vgl. die Darstellungen in Anhang B. Somit ist die Anforderung FMT_MSA.3.2/AK.TLS implizit erfüllt.

FTP_ITC.1/AK.FD
Inter-TSF trusted channel / Zum Fachdienst

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 mit dem Sperrstatus (OCSP) „good“**[104] **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	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/AK.FD	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 36	„Fachdienst“ beinhaltet in diesem Zusammenhang auch den Intermediär, da der TOE keine unmittelbare Verbindung zum Fachdienst aufbaut.
ST-Anwendungshinweis 37	TIP1-A_7254 wird umgesetzt durch das Refinement in FTP_ITC.1.1/AK.FD.

FTP_ITC.1/AK.VZD
Inter-TSF trusted channel / Zum zentralen Verzeichnisdienst

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 mit dem Sperrstatus (OCSP) „good“**[105] **gegenüber dem EVG ~~its end points~~** and protection of the channel data from modification **and ~~or~~** disclosure.
FTP_ITC.1.2/AK.VZD	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[104] Refinement: *Vgl. ST-Anwendungshinweis 37*
[105] Refinement: *Vgl. ST-Anwendungshinweis 37*

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“
ST-Anwendungshinweis 38	TIP1-A_7254 wird umgesetzt durch das Refinement in FTP_ITC.1.1/AK.VZD.

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

FTP_ITC.1.1/AK.KSR	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/AK.KSR	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/AK.KSR	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1/AK.TSL
Inter-TSF trusted channel / Zum TSL-Dienst

FTP_ITC.1.1/AK.TSL	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/AK.TSL	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/AK.TSL	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1/AK.CS
Inter-TSF trusted channel / Clientsystem

FTP_ITC.1.1/AK.CS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/AK.CS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/AK.CS	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1/AK.eHKT

Inter-TSF trusted channel / eHKT

FTP_ITC.1.1/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1.2/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1.3/AK.eHKT — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.3.3.8. Sicherer Datenspeicher

FDP_ACC.1/AK.SDS

Subset access control / Sicherer Datenspeicher

FDP_ACC.1.1/AK.SDS — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.SDS

Security attribute based access control / Sicherer Datenspeicher

FDP_ACF.1.1/AK.SDS — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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 Sicherheitsattribut „Administratorobjekt“ darf nur innerhalb einer Administratorsitzung entschlüsselt und gelesen und verschlüsselt und geschrieben werden, aber nicht außerhalb der Administratorsitzung gespeichert werden,

(5) Keine weiteren Regeln[106].

[106] Assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*

ST-Anwendungshinweis 39

TIP1-A_5484 wird umgesetzt durch Unterpunkt FDP_ACF.1.1/AK.SDS(3) in Kombination mit *KoCoBox MED+ OPB 2.1 Konnektor* [KoCo AGD_Kon-Sec, Abschnitt 3.4].

FDP_ACF.1.3/AK.SDS

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[107].

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 Sicherheitsattribut „Adminstratorobjekt“ weder lesen noch entschlüsseln.

(2) Das S_AK darf keine Datenobjekte des SDS mit dem Sicherheitsattribut „Adminstratorobjekt“ speichern oder modifizieren.

(3) none[108].

ST-Anwendungshinweis 40

Das Schutzprofil fordert die Modellierung eines Sicherheitsattributs zur Abgrenzung „allgemeiner Datenobjekte“ (die vom Anwendungskonnektor gelesen/geschrieben werden dürfen) und „Administratorobjekte“ (die nur im Kontext einer „Administratorsitzung“ gelesen/-geschrieben werden dürfen). Die KoCoBox MED+ setzt dieses Konzept so um, dass ausschließlich „allgemeine Datenobjekte“ existieren. Folglich gibt es kein Sicherheitsattribut, um Datenobjekte voneinander abzugrenzen. Auch Konfigurationsdaten, die im Rahmen einer Administratorsitzung geschrieben werden, gelten als „allgemeine Datenobjekte“.

Hintergrund dafür ist die in FDP_ACF.1.4/AK.SDS(1) formulierte Zugriffsregel. Diese verbietet dem Anwendungskonnektor explizit, „Administratorobjekte“ zu lesen. Die Dienste, die die Konfiguration anwenden müssen, sind jedoch Teil des Anwendungskonnektors, unterliegen also den Modellierungsregeln für S_AK und dürfen folglich die Daten gar nicht anwenden. Der TOE ließe sich nicht ohne einen angemeldeten Administrator starten.

Anwendungshinweis 188 des Schutzprofils fordert eine Darstellung, wie der Inhalt des sicheren Datenspeichers bei ausgeschaltetem Konnektor geschützt wird und wie die Initialisierung des sicheren Datenspeichers erfolgt.

Der sichere Datenspeicher ist nach FCS_COP.1/Storage.AES transparent verschlüsselt und nach FCS_COP.1/Sign durch Signaturen in der Integrität geschützt. Siehe auch SF.SecureStorage und SF.CryptographicServices/NK.

[107] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[108] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*

Das benötigte Schlüsselmaterial wird mit Hilfe der gSMC-K erzeugt oder ist auf der jeweils genutzten gSMC-K vorhanden. Der sichere Datenspeicher wird bei Erstinitiliasierung bereits in der Produktion durch den TOE eingerichtet.

6.3.3.9. Fachmodule

FDP_ACC.1/AK.VSDM
Subset access control / VSDM

FDP_ACC.1.1/AK.VSDM — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.9] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FDP_ACF.1/AK.VSDM
Security attribute based access control / VSDM

FDP_ACF.1.1/AK.VSDM — Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.9] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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 den 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) Keine weiteren Regeln.[109]

FDP_ACF.1.3/AK.VSDM — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None[110].

FDP_ACF.1.4/AK.VSDM — The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None[111].

[109] Assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
[110] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[111] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*

FMT_MSA.1/AK.VSDM
Management of security attributes / VSDM

FMT_MSA.1.1/AK.VSDM	The TSF shall enforce the VSDM-SFP to restrict the ability to *no operation*[112] the security attributes none[113] to S_Administrator.
ST-Anwendungshinweis 41	Das PP definiert für das Subjekt S_VSDM_Fachmodul lediglich die Identität – also den eindeutigen Namen des Fachmoduls – als Sicherheitsattribut (vgl. [BSI-CC-PP-0098, Tabelle 12]). Neben der Identität werden keine weiteren Sicherheitsattribute für das Fachmodul VSDM definiert, die durch einen Administrator geändert werden können. Daher werden hier keine Operationen und keine Sicherheitsattribute operationalisiert.

FMT_MSA.3/AK.VSDM
Static attribute initialization / VSDM

FMT_MSA.3.1/AK.VSDM	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.9] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FMT_MSA.3.2/AK.VSDM	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.9] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 42	Es gibt keine vom Administrator änderbaren Konfigurationswerte. Folglich können keine alternativen Anfangswerte definiert werden. Somit ist die Anforderung implizit erfüllt.

6.3.3.10. Übergreifende Sicherheitsanforderungen

FMT_MSA.4/AK
Security attribute value inheritance

FMT_MSA.4.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.10] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 43	Zur Interpretation des Begriffs „Verschlüsselungsrichtlinie“ vgl. ST-Anwendungshinweis 30 auf Seite 85.

FDP_RIP.1/AK
Subset residual information protection

FDP_RIP.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.3.10] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[112] Selection: ***create***, *change_default, query, modify, delete, [assignment: other operations]*
[113] Assignment: *list of security attributes*

6.3.4. Klasse FMT: Sicherheitsmanagement

FMT_SMR.1/AK
Security roles

FMT_SMR.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FMT_SMR.1.2/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_SMF.1/AK
Specification of Management Functions

FMT_SMF.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FMT_MOF.1/AK
Management of security functions behaviour

FMT_MOF.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
ST-Anwendungshinweis 44	Die gematik Spezifikation sieht die Betriebseigenschaft *MGM_LOGICAL_SEPARATION* nicht länger vor [gemSpec_Kon]. Die logische Trennung ist nicht im TOE implementiert ist. Daher ist es nicht möglich, die Auswahl „logische Trennung“ zu aktivieren.

FMT_MTD.1/AK.Admin
Management of TSF data / Administration

FMT_MTD.1.1/AK.Admin — The TSF shall restrict the ability to

(1) set, query, modify and delete the roles from other users,

(2) **set, modify and delete the authentication credentials for administrators,**

(3) **set and modify the Arbeitsplatzkonfiguration with assigned Clientsystem and eHealth-Kartenterminals,**

(4) **set and modify the Zeitpunkten und Gültigkeitsdauer der Prüfungsergebnisse zur Gültigkeit qualifizierter Zertifikate für die Erzeugung ordnungsgemäßer qualifizierten elektronischen Signaturen,**

(5) **change_default of the gültigen Signaturrichtlinie für automatische Signaturerzeugung,**

(6) **change_default of the gültigen Signaturrichtlinie für automatische Signaturprüfung,**

(7) **modify the configuration parameter to activate or deactivate the automatic installation of software updates,**

(8) **import the update data for Karten-Terminals and execute the update,**

(9) **configure the loggable system events,**

(10) **export and import the configuration data of the TOE,**

(11) **set and modify the maximum lifetime of OCSP cache entries,**

(12) **set and modify the keys of the sicheren Datenspeichers**,

(13) **set and import and export the X.509 certificates of Clientsystemen,**

(14) **reset to factory settings of ~~the~~ all TSF data (factory reset),**

(15) **import the CA certificates of an encryption PKI,**

(16) **query the version information of Fachmodule,**

(17) **modify the connection parameters of Clientsysteme,**

(18) **query the available smart cards of types eGK and HBA,**

(19) **query the expiry date of certificates on smart cards of types eGK and HBA,**

(20) **modify the PIN management parameters of SMC-B**

to administrator.

ST-Anwendungshinweis 45 FMT_MTD.1.1/AK.Admin(5), (6) kommt in der Architektur des vorliegenden TOE nicht zum Tragen, vgl. FMT_MSA.3/AK.Sig.

ST-Anwendungshinweis 46 Der TOE unterstützt die automatische Anwendung von Update-Paketen nicht.

ST-Anwendungshinweis 47 FMT_MTD.1.1/AK.Admin(12): Die Schlüssel des sicheren Datenspeichers werden beim ersten Start des Geräts – noch in der Fertigungsstraße – erzeugt und können ausschließlich im Rahmen des Werksresets neu generiert werden. Der TOE stellt kein Schlüsselzugriffsinterface bereit. Ein Werksreset wiederum kann nur vom Administrator ausgelöst werden. Somit ist (12) durch (14) implizit erfüllt.

ST-Anwendungshinweis 48 TIP1-A_7255 wird von FMT_MTD.1.1/AK.Admin(16) umgesetzt.

FMT_MTD.1/AK.Zert
Management of TSF data / Zertifikatsmanagement

FMT_MTD.1.1/AK.Zert — Die in [BSI-CC-PP-0098, Abschnitt 6.3.4] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

ST-Anwendungshinweis 49

(1) Der TOE löscht keine öffentlichen Schlüssel der CVC Root CA auf der gSMC-K. Der TOE initiiert die Übernahme öffentlicher Schlüssel der CVC Root CA aus übergebenen Cross-CV-Zertifikaten durch die gSMC-K.

Wenn der für die CA-Zertifikatsprüfung zu selektierende CVC-Root-Key auf der gSMC-K nicht vorhanden ist, werden mit dem Kartenkommando PSO VERIFY CERTIFICATE ausgewählte Cross-CV-Zertifikate zur Prüfung an die gSMC-K gesendet. Dadurch wird jeweils der im Cross-CV-Zertifikat enthaltene öffentliche CVC-Root-Key an die gSMC-K übertragen. Die gSMC-K verwaltet den erforderlichen Speicherplatz auf der Karte selbst und entfernt „unwichtige“ Einträge falls die Menge an importierten Schlüsseln die Kapazität der Karte übersteigt.

(2) Im TOE erfolgt ein Import, aber keine permanente Speicherung der öffentlichen Schlüssel der CVC Root CA. Die Schlüssel werden nur temporär im Rahmen der Zertifikatsprüfung verwendet.

6.3.5. Klasse FPT: Schutz der TSF

FPT_TDC.1/AK
Inter-TSF basic TSF data consistency

FPT_TDC.1.1/AK — The TSF shall provide the capability to consistently interpret

(1) Zertifikaten für die Prüfung qualifizierter elektronischer Signaturen,

(2) nicht-qualifizierter X.509-Signaturzertifikaten,

(3) X.509-Verschlüsselungszertifikaten,

(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) *Signaturrichtlinie*[114]

[114] Selection: *Signaturrichtlinie, Verschlüsselungsrichtlinie*

when shared between the TSF and another trusted IT product.

ST-Anwendungshinweis 50 — TIP1-A_5482 wird umgesetzt durch Unterpunkt FPT_TDC.1.1/AK(4).

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.

(3) Die Gültigkeit der X.509-Signaturzertifikate der SMC-B gemäß [gemSpec_SMC-B_ObjSys] muss gemäß Schalenmodell bis zu einem gültige CA-Zertifikat der ausstellenden (zugelassenen) CA, das in einer gültigen TSL enthalten ist, erfolgreich geprüft sein.

(4) Die Gültigkeit der X.509-Verschlüsselungszertifikate gemäß Schalenmodell bis zu einem gültige CA-Zertifikat der ausstellenden (zugelassenen) CA, das in einer gültigen TSL enthalten ist, erfolgreich geprüft sein.

(5) Die Gültigkeit der CVC gemäß [BSI-CC-PP-0082-2] 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 und CRL darf nur durch eine gültige TSL verteilt werden.

(9) *für Signaturrichtlinie die Kette der Signaturen bis zu einer bekannten Wurzelinstanz und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen*[115].

[115] Selection: *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*

(10) **Falls bei einer Zertifikatsprüfung OCSP-Abfragen verwendet werden, muss die Festlegung zeitlicher Toleranzen in einer OCSP-Response, definiert in GS-A_5215 [gemSpec_PKI, Abschnitt 9.1.2.2], bei der Interpretation verwendet werden.**[116]

when interpreting the TSF data from another trusted IT product.

FPT_FLS.1/AK
Failure with preservation of secure state

FPT_FLS.1.1/AK — The TSF shall preserve a secure state **according to [gemSpec_Kon, TAB_KON_504]** when the following types of failures occur:

(1) according to [gemSpec_Kon, TAB_KON_503] with type „SEC“ and severity „fatal“.

(2) Keine weiteren Fehlerarten[117]

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.

FPT_TEE.1/AK
Testing of external entities

FPT_TEE.1.1/AK — Die in [BSI-CC-PP-0098, Abschnitt 6.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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, und der geforderten Rolle 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 die unbekannte Karte kennzeichnen und weitere Aktionen mit dieser Karte verbieten[118].

[116] Refinement: *Anforderung aus GS-A_5215 in Anhang D*
[117] Assignment: *list of additional types of failures in the TSF*
[118] Assignment: *action for unknown smart cards*

FPT_TST.1/AK.Run-time
TSF testing / Normalbetrieb

FPT_TST.1.1/AK.Run-time	The TSF shall run a suite of self tests beim Anlauf und regelmäßig während des Normalbetriebs to demonstrate the correct operation of stored TSF executable code[119].
FPT_TST.1.2/AK.Run-time	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF configuration data[120].
FPT_TST.1.3/AK.Run-time	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[121].
ST-Anwendungshinweis 51	Die Sicherheitsanforderung FPT_TST.1 existiert bereits in einer Iteration für den Netzkonnektor, vgl. FPT_TST.1/NK.

FPT_TST.1/AK.Out-Of-Band
TSF testing / Out-Of-Band

FPT_TST.1.1/AK.Out-Of-Band	Die in [BSI-CC-PP-0098, Abschnitt 6.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FPT_TST.1.2/AK.Out-Of-Band	Die in [BSI-CC-PP-0098, Abschnitt 6.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
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 **the whole TSF**[122].

FPT_STM.1/AK
Reliable time stamps

FPT_STM.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.5] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.3.6. Klasse FAU: Sicherheitsprotokollierung

FAU_GEN.1/AK
Audit data generation

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**;

[119] Assignment: *parts of TSF*
[120] Assignment: *parts of TSF data*
[121] Assignment: *parts of TSF*
[122] Assignment: *parts of TSF mit gespeichertem ausführbarem TSF-Code*

b) All auditable events for the *not specified*[123] 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,
- Ereignisse vom Typ „Sec“ der Fachmodule[124].

FAU_GEN.1.2/AK

The TSF shall record within each audit record at least the following information:

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

b) For each **specified** audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no further information[125].

ST-Anwendungshinweis 52

Anwendungshinweis 203 des Schutzprofils bildet die Brücke zu TIP1-A_4710. Diese Anforderung bestimmt, dass keine persönlichen oder medizinischen Daten protokolliert werden dürfen.

Der Anwendungshinweis wird um die Nennung von „Schlüsselmaterial“ verfeinert, um die Anforderung VSDM-A_2789 zu erfüllen:

> 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 **oder Schlüsselmaterial** enthalten. Zum Nachweis dieser Anforderung für die Produktzulassung sind alle möglichen Protokoll-Einträge zu dokumentieren. Die Spezifikation Konnektor [gemSpec_Kon] gibt im Anhang F eine Übersicht der Ereignisse (Events), wobei nur die Beschreibungen der Ereignisse für die jeweiligen Technischen Anwendungsfülle (TUC) verbindlich sind.

[123] Selection: *choose one of: minimum, basic, detailed, not specified*
[124] Assignment: *additional events*
[125] Assignment: *other audit relevant information*

FAU_SAR.1/AK
Audit review

FAU_SAR.1.1/AK	The TSF shall provide administrators[126] with the capability to read the system log and the security log[127] from the audit records.
FAU_SAR.1.2/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FAU_STG.1/AK
Protected audit trail storage

Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 fulfilled in this Security Target by FAU_GEN.1/NK.SecLog
FAU_STG.1.1/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FAU_STG.1.2/AK	Die in [BSI-CC-PP-0098, Abschnitt 6.3.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FAU_STG.4/AK
Prevention of audit data loss

Hierarchical to:	FAU_STG.3
Dependencies:	FAU_STG.1 fulfilled in this Security Target by FAU_STG.1/AK
FAU_STG.4.1/AK	The TSF shall overwrite the oldest stored audit records and take no further action[128] if the audit trail is full. **The TOE reserves memory in the non-volatile NAND flash for the event log. If the size of the log exceeds 80% of the reserved memory, the TOE shall inform the administrator via the display.**
ST-Anwendungshinweis 53	Das Überschreiben des ältesten Log-Eintrags aus dem PP-Assignment wird durch die Konfigurationsparameter *LOG_DAYS* (für den Basiskonnektor) und *FM_<fmName>_LOG_DAYS* (für Fachmodule) gesteuert. Die Parameter geben an, nach wievielen Tagen Logeinträge frühestens überschrieben werden können. Sollte die diese Grenze an Tagen noch nicht erreicht sein und das Protokoll trotzdem voll sein, werden die ältesten Einträge gelöscht und der Konnektor wird spezifikationskonform in den Fehlerzustand *EC_LOG_OVERFLOW* versetzt.

[126] Assignment: *authorised users*
[127] Assignment: *list of audit information*
[128] Assignment: *other actions to be taken in case of audit storage failure*

6.4. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit für dieses Security Target entsprechen denen, die in [BSI-CC-PP-0097] und [BSI-CC-PP-0098] definiert sind.

6.4.1. Verfeinerung zur Vertrauenswürdigkeitskomponente ADV_ARC.1

Die Verfeinerungen in [BSI-CC-PP-0098; BSI-CC-PP-0097] gelten ohne Anpassung.

6.4.2. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_OPE.1

Die Verfeinerungen in [BSI-CC-PP-0098; BSI-CC-PP-0097] gelten ohne Anpassung.

6.4.3. Verfeinerung zur Vertrauenswürdigkeitskomponente ALC_DEL.1

Die Verfeinerungen in [BSI-CC-PP-0098; BSI-CC-PP-0097] gelten ohne Anpassung.

6.4.4. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_PRE.1

Die Verfeinerungen in [BSI-CC-PP-0098; BSI-CC-PP-0097] gelten ohne Anpassung.

6.4.5. Verfeinerung für die Integration der Fachmodule NFDM und AMTS

Der Konnektor berherbergt die Fachmodule NFDM und AMTS, die nicht im Rahmen der CC-Zertifizierung betrachtet, sondern nach Technischen Richtlinien zertifziert werden. Dennoch haben diese Fachmodule Auswirkungen auf den Gesamtkonnektor, indem Sie Forderungen an Eigenschaften des Konnektors stellen. Der zertifizierte Konnektor muss diese Eigenschaften aufweisen. Um sicherzustellen, dass die Zertifizierung des Konnektors diese Eigenschaften berücksichtigt, gelten die folgende Verfeinerungen. ASE_TSS wird wie folgt verfeinert:

> **Der Konnektor unterstützt die Fachmodule NFDM und AMTS. In den Technischen Richtlinien TR-03154 [TR-03154] und TR-03155 [TR-03155], Kapitel 3.3.2 werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die für die Fachmodule NFDM und AMTS relevanten Sicherheitseigenschaften des Konnektors müssen zusätzlich im Security Target des Konnektors aufgenommen werden.**
>
> **Der *Hersteller* muss im Security Target beschreiben, dass der Konnektor die nach [TR-03154] und TR-03155 [TR-03155], Kapitel 3.3.2 relevanten Sicherheitseigenschaften des Konnektors umsetzt.**
>
> **Der *Evaluator* muss prüfen, ob die nach [TR-03154] und TR-03155 [TR-03155], Kapitel 3.3.2 relevanten Sicherheitseigenschaften des Konnektors vollständig im Security Target berücksichtigt sind.**

ADV_FSP wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM und AMTS. In den Technischen Richtlinien TR-03154 [TR-03154] und TR-03155 [TR-03155], Kapitel 3.3.2 werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die dabei von den Fachmodulen aufgerufenen Schnittstellen des Anwendungskonnektors müssen beschrieben werden.

Der *Hersteller* muss eine Beschreibung der Schnittstellen des Anwendungskonnektors bereitstellen, an denen die relevanten Sicherheitseigenschaften des Konnektors umgesetzt werden.

Der *Evaluator* muss die Beschreibung der Schnittstellen des Anwendungskonnektors, an denen die relevanten Sicherheitseigenschaften des Konnektors umgesetzt werden auf Vollständigkeit hinsichtlich der Vorgaben in den Technischen Richtlinien prüfen.

Die Prüfung der sicheren und korrekten Implementierung der von den Schnittstellen bereitgestellten relevanten Sicherheitseigenschaften des Konnektors wird durch die Verfeinerung von ADV_TDS gefordert. ADV_TDS wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM und AMTS. In den Technischen Richtlinien TR-03154 [TR-03154] und TR-03155 [TR-03155], Kapitel 3.3.2 werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften muss geprüft werden.

Der *Hersteller* muss ausreichende Nachweise bereitstellen, die es erlauben die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften zu prüfen.

Der *Evaluator* muss die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften prüfen.

Die Nachweise des Herstellers können zum Beispiel eine Beschreibung der von den Fachmodulen aufgerufenen Schnittstellen und die Abbildung der relevanten TUCs auf den Source Code enthalten. Im Rahmen der Evaluierung kann auch auf andere Prüfaspekte, wie zum Beispiel ADV_FSP, ADV_IMP oder ATE verwiesen werden, wenn darin entsprechende Prüfnachweise erbracht wurden

6.5. Erklärung der Sicherheitsanforderungen

6.5.1. Erklärung der Abhängigkeiten der SFR des Netzkonnektors

Die Abhängigkeiten der in Abschnitt 6.2 aufgestellten funktionalen Sicherheitsanforderungen sind erfüllt. Es gelten dieselben Auflösungen von Abhängigkeiten, wie sie im Schutzprofil [BSI-CC-PP-0097, Abschnitt 6.4.2] beschrieben sind.

Die Abhängigkeiten der aus dem Schutzprofil des Gesamtkonnektors [BSI-CC-PP-0098] übernommenen Sicherheitsanforderungen sind dem Schutzprofil zu entnehmen.

Die Abhängigkeiten der über die Schutzprofile hinaus aufgenommenen Sicherheitsanforderungen sind bei der Definition des jeweiligen SFR notiert. Die zusätzlich aufgenommenen SFR sind Iterationen bestehender Komponenten, sodass sich durch diese keine neuen Abhängigkeiten ergeben.

Die in Abschnitt 5.1 neu eingeführte Komponente FCS_RNG.1 hat keine Abhängigkeiten, die aufgelöst werden müssen.

6.5.2. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors

Die Zuordnung von Sicherheitszielen zu Sicherheitsanforderungen entspricht weitestgehend der Zuordnung, die in [BSI-CC-PP-0098; BSI-CC-PP-0097] getroffen wurde.

Die in diesem Security Target neu hinzugefügten Sicherheitsziele werden ebenfalls auf die Sicherheitsanforderungen abgebildet. Gleiches gilt für die neu eingeführten Sicherheitsanforderungen, die den Sicherheitszielen zugeordnet werden müssen. Tabelle 6.3 auf Seite 108 ordnet diese neuen Abbildungen in den Kontext der im Schutzprofil vorgenommenen Zuordnungen ein. Dabei ist die Legende aus Tabelle A.1 (auf Seite 146) zu verwenden.

Die Einführung der zusätzlichen Sicherheitsanforderungen wird wie folgt begründet:

FCS_COP.1/Sign wurde hinzugefügt, um die Algorithmen des TOE zur Signaturerstellung und -verifikation zu repräsentieren. Die Algorithmen tragen dazu bei, die Schutzziele O.NK.Schutz, O.NK.EVG_Authenticity und O.NK.VPN_Auth zu erfüllen, indem sie für die Prüfung der Integrität von Hashes, der Integrität der TSL/CRL und der VPN-Vertrauensanker herangezogen werden.

FCS_COP.1/Storage.AES helfen, die Benutzerdaten und den TOE selbst zu schützen, wie von O.NK.Schutz vorgesehen.

FCS_RNG.1/Hash_DRBG trägt dazu bei, dass beim TLS-Verbindungsaufbau sichere Zufallszahlen verwendet werden. Dadurch wird das Schutzziel O.NK.TLS_Krypto erfüllt.

6.5.3. Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors

Die detaillierte Erklärung der Sicherheitsziele des Netzkonnektors wird unverändert aus [BSI-CC-PP-0098; BSI-CC-PP-0097] übernommen.

	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	.	.	.	.	.	.	✓	.	✓	✓	.	.	.
FTP_ITC.1/NK.VPN_SIS	.	.	.	.	.	.	✓	.	✓	✓	.	.	.
FDP_IFC.1/NK.PF	.	.	.	.	.	.	.	.	.	.	✓	✓	✓
FDP_IFF.1/NK.PF	.	.	.	.	.	.	.	.	.	.	✓	✓	✓
FMT_MSA.3/NK.PF	.	.	.	.	.	.	.	.	.	.	✓	✓	.
FPT_STM.1/NK	.	.	.	.	✓	✓	.	.	.	.	.	.	.
FPT_TDC.1/NK.Zert	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_RIP.1/NK	.	✓	.	.	.	.	.	.	.	.	.	.	.
FPT_TST.1/NK	.	✓	.	.	.	.	.	.	.	.	.	.	.
FPT_EMS.1/NK	.	✓	.	.	.	.	.	.	✓	✓	.	.	.
FAU_GEN.1/NK.SecLog	.	.	.	.	✓	.	.	.	.	.	.	.	.
FAU_GEN.2/NK.SecLog	.	.	.	.	✓	.	.	.	.	.	.	.	.
FMT_SMR.1/NK	✓	.	.	✓	.	.	.	.	.	.	✓	✓	.
FMT_MTD.1/NK	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_UID.1/NK.SMR	.	.	.	✓	.	.	.	.	.	.	.	.	.
FTP_TRP.1/NK.Admin	✓	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_SMF.1/NK	✓	.	.	✓	.	.	.	.	.	.	✓	✓	.
FMT_MSA.1/NK.PF	.	.	.	✓	.	.	.	.	.	.	✓	✓	.
FMT_MSA.4/NK	.	.	.	✓	.	.	.	.	.	.	.	.	.
FCS_COP.1/NK.Hash	.	✓	.	.	.	.	.	.	.	✓	.	.	.
FCS_COP.1/NK.HMAC	.	.	.	.	.	.	.	.	.	✓	.	.	.
FCS_COP.1/NK.Auth	.	✓	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/NK.ESP	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/NK.IPsec	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_CKM.1/NK	.	✓	✓	.	.	.	✓	.	✓	✓	.	.	.
FCS_CKM.2/NK.IKE	.	.	.	.	.	.	✓	.	✓	✓	.	.	.
FCS_CKM.4/NK	✓	✓	✓	.	.	.	✓	.	✓	✓	.	.	.
FTP_ITC.1/NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.
FPT_TDC.1/NK.TLS.Zert	✓	.	.	.	.	.	.	.	.	.	.	.	.
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.1/NK.Zert	✓	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ITC.2/NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ETC.2/NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.
FMT_MOF.1/NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.

Abbildung der Sicherheitsziele des NK auf Sicherheitsanforderungen

	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
FDP_ACF.1/AK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_RNG.1/Hash_DRBG	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/Storage.AES	.	✓	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/Sign	.	✓	✓	.	.	.	✓	.	.	.	.	.	.

Tabelle 6.3.: Abbildung der Sicherheitsziele des NK auf Sicherheitsanforderungen

6.5.4. Erklärung der Abhängigkeiten der SFR des Anwendungskonnektors

Die Abhängigkeiten der in Abschnitt 6.3 aufgestellten funktionalen Sicherheitsanforderungen sind erfüllt. Es gelten dieselben Auflösungen von Abhängigkeiten, wie sie im Schutzprofil [BSI-CC-PP-0098, Abschnitt 6.5.2] beschrieben sind.

6.5.5. Überblick der Abdeckung von Sicherheitszielen des Anwendungskonnektors

Die Zuordnung von Sicherheitszielen zu Sicherheitsanforderungen des Anwendungskonnektors entspricht der Zuordnung, die im Schutzprofil getroffen wurde [BSI-CC-PP-0098, Abschnitt 6.5.4].

6.5.6. Detaillierte Erklärung für die Sicherheitsziele des Anwendungskonnektors

Die detaillierte Erklärung der Sicherheitsziele des Anwendungskonnektors wird unverändert aus [BSI-CC-PP-0098] übernommen.

6.6. Erklärung für Erweiterung der Sicherheitsanforderungen

FCS_RNG.1/Hash_DRBG
Die Sicherheitsanforderung FCS_RNG.1/Hash_DRBG wurde eingeführt, um die Anforderungen der ebenfalls eingeführten Komponente FCS_RNG.1 zu präzisieren. Die Erklärung für die Einführung der Familie FCS_RNG in Abschnitt 5.1 gilt auch für das resultierende SFR FCS_RNG.1/Hash_DRBG. Die Sicherheitsanforderung erfüllt das Sicherheitsziel O.NK.TLS_Krypto, vgl. auch Abschnitt 6.5.1.

FIA_API.1/AK.TLS
Die Sicherheitsanforderung FIA_API.1/AK.TLS wurde eingeführt, um die Anforderung gs-a_4384 zu erfüllen, die fordert, dass der Konnektor sich mit einem X.509 Zertifikat identifizieren muss, wenn er Server in einer TLS-Verbindung ist. Die Sicherheitsanforderung erfüllt das Sicherheitsziel O.AK.LAN.

FIA_SOS.1/AK.CS.Passwörter

Die Sicherheitsanforderung FIA_SOS.1/AK.CS.Passwörter wurde eingeführt, da die Qualitätsmetriken für Passwörter an der Clientsystemschnittstelle unterschiedlich sind und sich FIA_SOS.1/AK.Passwörter explizit auf die Passwörter an der Managementschnittstelle bezieht. Die Sicherheitsanforderung erfüllt das Sicherheitsziel O.AK.LAN.

6.7. Erklärung für die gewählte EAL-Stufe

Die Erklärung der gewählten EAL-Stufe wird unverändert aus dem Schutzprofil [BSI-CC-PP-0098] übernommen.

7. ASE_TSS: Basiskonnektor

Dieses Kapitel vermittelt einen Überblick über die IT-Sicherheitsfunktionen des TOE, wie sie in der funktionalen Spezifikation beschrieben sind. Es enthält Beschreibungen der allgemeinen technischen Verfahren, die der TOE anwendet, um die Sicherheitsanforderungen zu erfüllen.

Das Kapitel ist gegliedert in Funktionen, die vom Netzkonnektor (Abschnitt 7.1) und Funktionen, die vom Anwendungskonnektor erbracht werden. Der Abschnitt über die Funktionen des Netzkonnektors ist dessen Security Target [KoCo ASE_ST-97] entnommen.

Die beiden Abschnitte 7.3 und 7.4 zeigen tabellarisch die Zusammenhänge zwischen den Sicherheitsfunktionen des TOE und den Sicherheitsanforderungen, die dieses Security Target in den Abschnitten 6.2 (für den Netzkonnektor) und 6.3 (für den Anwendungskonnektor) aufstellt. Auch hier sind die NK-spezifischen Angaben aus dem Security Target des NK übernommen.

Dieses Kapitel beschreibt die Funktionalität des Basiskonnektors. Das Folgekapitel setzt ASE_TSS fort, indem die Anforderungen der Fachmodule an den TOE beschrieben werden und aufgelistet wird, wie der TOE diese Anforderungen erfüllt. Das Folgekapitel gehört somit formal zum zu prüfenden Umfang des Security Targets.

7.1. TOE Sicherheitsfunktionen des Netzkonnektors

7.1.1. VPN-Client (SF.VPN)

Die Sicherheitsfunktion SF.VPN erstellt sichere Kommunikationskanäle zwischen dem TOE und einem entfernten, vertrauenswürdigen IT-Produkt. Dazu wird eine IKEv2 Implementierung verwendet. Diese Kanäle sind logisch von anderen Kommunikationskanälen separiert. Sie bieten gesicherte Identifizierung der Endpunkte und Schutz der über den Kanal übertragenen Daten vor Manipulation und Preisgabe. Solche Kanäle werden vom Konnektor für Verbindungen in die Telematikinfrastruktur und zum SIS verwendet. Der TOE verwendet die Identität auf der gSMC-K#1, um sich gegnüber den entfernten VPN-Konzentratoren zu authentisieren.

Umgesetzte SFR	
FTP_ITC.1/NK.VPN_SIS	FTP_ITC.1/NK.VPN_TI

Zertifikate werden sowohl mathematisch geprüft, als auch gegen eine TSL und eine CRL geprüft. Die Signaturen der TSL und der CRL werden ebenfalls vom TOE geprüft. Beide Listen werden alle 24 Stunden über einen HTTP-Download aktualisiert.

Darüberhinaus verfolgt der TOE die Ablaufdaten kryptographischer Algorithmen. Wenn die Algorithmen ablaufen, wird der TOE seine Operation einstellen und nicht mehr funktional sein. Die Ablaufdaten und die Algorithmen sind ausschließlich über Software-Updates möglich.

Die vorliegende Implementierung unterstützt IPsec, wie von [gemSpec_Kon] gefordert: IKEv2 [RFC 7296] ohne herstellerspezifische Erweiterungen und Main Mode Exchange wird verwendet. NAT Traversierung wird unterstützt.

Umgesetzte SFR
FPT_TDC.1/NK.Zert

Wenn der TOE konfiguriert ist, sich mit der Telematikinfrastruktur zu verbinden, wird dise Verbindung automatisch aufgebaut, wenn dies technisch möglich ist (d.h. wenn der VPN-Konzentrator erreicht werden kann). Im Fehlerfall werden erneute Versuche verzögert, um nicht das Sicherheitsprotokoll mit Einträgen zu fluten. Wenn der TOE nicht für eine automatische Verbindung mit der Telematikinfrastruktur konfiguriert ist, wird keine Verbindung aufgebaut. Der Auf- und der Abbau einer VPN-Verbindung wird im Sicherheitslog protokolliert.

Um die zentrale Telematikinfrastruktur vor Angriffen zu schützen, ist die Kommunikation über den VPN-Kanal spezifischen Komponenten vorbehalten (durch SF.DynamicPacketFilter). Die einzigen Komponenten, denen der Datentransfer in die TI gestattet ist, sind der Anwendungskonnektor, Fachdienste, Clientsysteme und Dienste für Namensauflösung (DNS), Zeitabgleich (NTP) und der Download von TSL, CRL und BNetzAVL.

7.1.2. Dynamischer Paketfilter (SF.DynamicPacketFilter)

Die Sicherheitsfunktion SF.DynamicPacketFilter stellt eine Firewall (regelbasierten, dynamischen Paketfilter) für Netzwerkverbindungen über die LAN- und WAN-Schnittstellen des Konnektors zur Verfügung. Die Firewall kann über Regeln konfiguriert werden, die Pakete filtern. Filterkriterien sind:

- IP Adressen (Quelle und Ziel),
- Portnummern (Quelle und Ziel),
- Protokolltypen,
- physische Schnittstellen (Quelle oder Ziel),
- die Netzwerkschnittstellen für Eintritt und Austritt der Daten (LAN, WAN, VPN),
- Verbindungsstatus

Umgesetzte SFR	
FDP_IFC.1/NK.PF	FDP_IFF.1/NK.PF

Das Standard-Regelset ist so gestaltet, dass es maximalen Schutz bietet. Dazu werden nur notwendige Verbindungen erlaubt. Um absichtliches und unabsichtliches Untergraben der TOE Sicherheitsmaßnahmen zu verhindern, dürfen ausschließlich Administratoren Firewallregeln hinzufügen. Auch hier sind die Möglichkeiten stark eingeschränkt. Der Administrator darf lediglich solche Regeln hinzufügen, die Kommunikation zwischen dem LAN und dem WAN erlauben. Es ist nicht möglich, Regeln einzuführen, die explizite Verbotsregeln des Standard-Regelsets aufheben. Die vom Administrator eingegebenen Regeln werden nach den Regeln des Standard-Regelsets bewertet. Neue Regeln werden über die Schnittstelle zum Anwendungskonnektor gesetzt.

Umgesetzte SFR	
FMT_MSA.3/NK.PF	FDP_IFC.1/NK.PF

Es ist möglich einen von zwei Betriebsmodi auszuwählen, für die unterschiedliche Regelsets definiert sind:

Serieller/Gateway Modus Der Konnektor wird zwischen dem lokalen Netzwerk und dem Internet-Gateway installiert. Der Zugang zum Internet wird in diesem Fall über das WAN-Interface PS.WAN bereitgestellt (*ANLW_ANBINDUNGS_MODUS = InReihe*).

Paralleler Modus Der Konnektor wird gemeinsam mit dem Internet-Gateway, den Clientsystemen und anderen Geräten als Teil des lokalen Netzwerks installiert. Der Zugang zum Internet wird in diesem Fall über das LAN-Interface PS.LAN bereit gestellt. Das WAN-Interface bleibt in diesem Fall ungenutzt (*ANLW_ANBINDUNGS_MODUS = Parallel*).

Darüber hinaus kann der Administrator auswählen, ob. bzw. wie den Clientsystemen der Zugang zum Internet ermöglicht werden soll. Es stehen drei Möglichkeiten zur Verfügung:

SIS Verkehr aus dem LAN wird über VPN SIS ins Internet geleitet (*ANLW_INTERNET_MODUS = SIS*)

IAG Verkehr aus dem LAN wird über das Internet Access Gateway ins Internet geleitet. Bedingt, dass der serielle/Gateway Modus aktiv ist (*ANLW_INTERNET_MODUS = IAG*).

Keiner Verkehr aus dem LAN wird nicht ins Internet geleitet (*ANLW_INTERNET_MODUS = Keiner*).

Die vordefinierten Sets an Filterregeln können nicht modifiziert oder entfernt werden, außer wenn die Policies durch ein Firmware-Update in den Konnektor eingebracht werden.

Umgesetzte SFR
FMT_MSA.1/NK.PF

Die vordefinierten Regelsets setzen die Anforderungen der Konnektor-Spezifikation um [gemSpec_Kon, Abschnitt 4.2.1.1.2].

Explizit erlaubt sind alle Verbindungen, von denen die Spezifikation fordert, dass der Konnektor sie erlauben muss.

Explizit verboten sind alle Verbindungen, von denen die Spezifikation fordert, dass der Konnektor sie unterbinden muss.

Die Firewall-Regeln stellen sicher, dass nur die Protokolle IPv4, ICMP (Netzwerkebene), TCP, UDP, ESP (Transportebene) für die Kommunikation mit der Telematikinfrastruktur erlaubt sind.

Die Routing-Tabellen des TOE stellen sicher, dass ausgehender Verkehr nur über LS.VPN_TI in die TI geleitet wird, wenn die Zieladresse Teil eines Subnetzes der TI oder Teil eines Bestandsnetzes ist. Jeglicher anderer Verkehr wird über LS.VPN_SIS, bzw. LS.LAN geleitet.

Der dynamische Paketfilter erlaubt dem TOE ebenfalls, Netzwerkpakete zu identifizieren, die weder zu einer bereits aufegebauten, noch zu einer im Aufbau befindlichen Verbindung gehören. Solche nicht-wohlgeformeten Pakete werden verworfen.

Der TOE führt Buch über den Status aller seiner Netzwerkverbindungen, sowie über deren relevante Informationen. Dafür setzt der TOE den Netfilter des Linux Kernels ein.

Das Hoch- und Herunterfahren des Paketfilters wird im Audit-Log des Konnektors protokolliert. Ebenso werden Informationen protokolliert, die für Basic Intrusion Prevention benötigt werden. Vorsichtsmaßnahmen sind implementiert, um zu verhindern, dass das Audit-Log mit speziell gefertigten Nachrichten geflutet wird. So könnte ein Angreifer versuchen, wichtige Nachrichten im Log zu überschreiben.

Umgesetzte SFR
FDP_IFF.1/NK.PF

7.1.3. Netzbasierte Sicherheitsfunktionen (SF.NetworkServices)

Die Sicherheitsfunktion SF.NetworkServices stellt dem TOE zuverlässige Zeitstempel zur Verfügung. Eine Referenzzeit wird über den VPN-Kanal von einem vertrauenswürdigen NTP-Server in der Telematikinfrastruktur bezogen. Dabei wird NTP in Version 4 verwendet [RFC 5905]. Die Abweichung zwischen der Netzwerkzeit und der lokalen Zeit im TOE darf maximal 1 Stunde betragen. Der TOE verwendet die Uhrzeit hauptsächlich, um die Gültigkeit von Zertifikaten zu prüfen und um Protokolleinträge mit Zeitstempel schreiben zu können. Die Synchronisation der Zeit mit dem NTP-Server findet nach dem Boot-Vorgang kontinuierlich statt. Die Intervalle zwischen den Synchronisationsabrufen betragen zwischen 64 und 1024 Sekunden, wie im NTP-Protokoll vorgesehen.

Umgesetzte SFR
FPT_STM.1/NK

Alle Anwendungen im TOE können über SF.NetworkServices die aktuelle Zeit erfragen. Der TOE stellt die Uhrzeit auch über seinen Zeitdienst an der Schnittstelle LS.LAN zur Verfügung (ebenfalls mit NTPv4). Cliensysteme und andere Nutzer im LAN des Leistungserbringers können den Zeitdienst verwenden.

Der TOE bietet weitere Netzwerkdienste für die Clientsysteme im LAN an:

- DHCP Server für die Konfiguration von Systemen mit IP-Adressen und Netzwerkparametern
- DNS Server für die Namensauflösung

7.1.4. Selbstschutz (SF.SelfProtection/NK)

Die Sicherheitsfunktion SF.SelfProtection/NK ist dafür verantwortlich, den TOE und die Daten, die er verarbeitet, vor Angriffen und Manipulation zu schützen.

Sensible Daten werden aus dem Arbeitsspeicher gelöscht, sobald sie nicht mehr verwendet werden. Das umfasst kryptographische Schlüssel, Session Keys, kurzlebige Schlüssel während des Ver- und Entschlüsselungsvorgangs, aber auch sensible Benutzerddaten. Das Löschen wird durch aktives Überschreiben der entsprechenden Speicherbereiche mit einer Konstante oder pseudo-zufälligen Werten umgesetzt.

Umgesetzte SFR	
FCS_CKM.4/NK	FDP_RIP.1/NK

Der TOE kann eine Reihe von Selbsttests ausführen, um seine Integrität und die Funktionsfähigkeit seiner eigenen Sicherheitsfunktionen und Komponenten zu beweisen. Abhängig von deren Ausprägung werden die Selbsttests entweder beim Systemstart, während des normalen Betriebs oder zu beiden Gelegenheiten ausgeführt. Der Administrator kann die Selbsttests ebenfalls starten. Folgende Selbsttests sind umgesetzt:

- Prüfung auf Integrität des sicheren Datenspeichers
- Prüfung auf Integrität des ausführbaren Codes der TOE Sicherheitsfunktionen.

Der sichere Datenspeicher speichert die Konfiguration des TOE in einem verschlüsselten Dateisystem. Die Integrität des sicheren Datenspeichers wird sichergestellt, indem für jede Datei des Dateisystems ein SHA-256 Hash berechnet, signiert und separat abgespeichert wird. Für die Signatur wird ein privater Schlüssel der gSMC-K verwendet. Beim Systemstart werden alle Hashwerte neu berechnet und mit den abgespeicherten Werten verglichen. Zusätzlich werden die Pfade und Namen aller Daten- und Signaturdateien in einem Journal abgelegt. Das Journal selbst wird ebenfalls signiert und mit einer Signaturdatei ergänzt. Die Signaturdateien für die Datendateien stellen sicher, das die Datendateien nicht manipuliert worden sind; das Journal stellt sicher, dass keine Daten entfernt oder hinzugefügt worden sind. Die Prüfung der Integrität der TSF kann ebenfalls vom Administrator durchgeführt werden. Weiterhin testet der TOE seine Integrität alle 24 Stunden selbst. ST-Anwendungshinweis 6 erweitert die Prüfung, sodass nicht nur ausführbare Dateien getestet werden, sondern auch alle anderen Teil der Firmware.

Die Integrität des Root-Dateisystems im NAND-Flash (Teil der TSF) wird sichergestellt, indem ein einzelner SHA-512 Hash über einer Hash-Datenbank verglichen wird. Die Hash-Datenbank wird beim Systemstart erstellt und enthält die Dateinamen und Hashes aller Daten im Root-Dateisystem. Wenn der Hash über der erstellten Datenbank mit einem abgespeicherten und signierten Hash übereinstimmt, gilt der Test als erfolgreich. Der Referenz-Hash wird mit einem dedizierten privaten Schlüssel signiert, der aus der PKI des Herstellers stammt. Die Signatur wird mit dem passenden öffentlichen Schlüssel mittels RSASSA-PSS verifiziert. Der Test wird während des Systemstarts und im laufenden Betrieb ausgeführt. Schlägt der Test während des Systemstarts fehl, bricht der TOE den Systemstart ab und hält an. Im Normalbetrieb führt der fehlschlagende Test dazu, dass der TOE seinen Dienst bis auf bestimmte Administrationsfunktionen einstellt. Die Tests werden von Skripten ausgeführt, die zweimal im System vorhanden sind: Für die Tests während des Systemstarts werden die Skripte aus dem Initramfs geladen, während des Normalbetriebs liegen sie im Root-Dateisystem.

Die Integrität des Linux Kernels und des Initramfs (Teile der TSF) wird durch den Boot-Loader sichergestellt. Der TOE verifiziert eine RSASSA-PKCS1-1.5 Signatur und prüft, dass die SHA-256 Hashes für den Kernel und das Initramfs mit den signierten Hashes korrespondieren. Der öffentliche Schlüssel für die Signaturverifikation ist im Boot-Loader abgespeichert.

Umgesetzte SFR
FPT_TST.1/NK

Der Boot-Loader (Teil der TSF) wird durch einen SHA-256 Hash und eine Signatur abgesichert, die vom SoC (Teil der Betriebsumgebung) verifiziert werden. Der öffentliche Schlüssel ist im Boot-Loader abgespeichert. Ein Hash des öffentlichen Schlüssels ist in einem einmalig beschreibbaren Speicherbereich des SoC gespeichert. Der Schlüssel wird im Produktionsprozess des Konnektors dort abgelegt. Dieser Hash wird ebenfalls verifiziert.

Für die Erstellung der Signaturen, die in den Integritätsprüfungen verwendet werden, setzt der TOE die gSMC-K ein.

Die Operationen und logischen Eigenschaften des TOE sind so implementiert, dass sie Seitenkanalattacken widerstehen. Der TOE stellt sicher, dass keine Informationen über die Netzwerkschnittstellen abfließen kann. Im Besonderen gilt dies für VPN-Sitzungsschlüssel, jegliches verwendete oder abgespeicherte Schlüsselmaterial und zu schützende Daten der TI und der Bestandsnetze.

Der TOE verwendet SELinux Policys, um zusätzlichen, verpflichtenden Zugriffsschutz (mandatory access control, MAC) für Ressourcen wie Dateien, Verzeichnisse, Sockets und Geräte zu erzwingen. Der TOE nutzt zusätzlich Code aus dem linux-hardened Project, um das System weiter zu härten (Verfeinerung von ADV_ARC.1).

Der TOE stellt sicher, dass der sichere Datenspeicher automatisch verschlüsselt wird (vgl. SF.CryptographicServices/NK). Zusätzlich prüft der TOE permanent die Zeitabweichung von maximal 1 Stunde zur Netzwerkzeit (vgl. SF.NetworkServices).

Umgesetzte SFR
FPT_EMS.1/NK

7.1.5. Protokollierungsdienst/NK (SF.Audit/NK)

Der TOE erzeugt Protokolleinträge für Ereignisse, die in FAU_GEN.1/NK.SecLog spezifiziert sind. Protokolleinträge enthalten die folgenden Informationen:

- Thema (Topic) des Ereignisses
- Datum und Uhrzeit des Ereignisses
- Art des Ereignisses
- Schweregrad
- Identität des auslösenden Subjekts (System oder die ID des korrespondierenden Fachmoduls)
- Ausgang (Erfolg oder Fehler) des Ereignisses, falls relevant
- Bei Konfigurationsänderungen: Benutzername des Administrators

Umgesetzte SFR	
FAU_GEN.1/NK.SecLog	FAU_GEN.2/NK.SecLog

7.1.6. Administration/NK (SF.Administration/NK)

Die Sicherheitsfunktionen des TOE definieren eine Rolle „Administrator“. Benutzer greifen zur Verwaltung des TOE über eine TLS-Verbindung auf den TOE zu und werden dabei vom Anwendungskonnektor authentisiert. Die TLS-Verbindung wird von der Funktion SF.CryptographicServices/NK bereit gestellt. Ist ein Administrator authentisiert, ist er autorisiert, verschiedene TSF-Parameter zu konfigurieren und folgende TSF-bezogene Operationen durchzuführen:

- Die Systemzeit/Echtzeituhr modifizieren

- Die Regeln des dynamischen Paketfilters anpassen (vgl. SF.DynamicPacketFilter und FMT_MSA.1/NK.PF)
- Das Sicherheitsprotokoll abfragen
- Die Selbsttests des Konnektors auslösen (vgl. SF.SelfProtection/NK)

Es ist zu beachten, dass die Web-Anwendung in der Umgebung des Konnektors ausgeführt wird. Die Sicherheitsleistungen werden von der Schnittstelle LS.LAN.HTTP_MGMT erbracht, die den Authentisierungsstatus des Administrators prüft.

Der TOE informiert den Administrator über kritische Betriebszustände über das Display an der Gehäusefront des Konnektors (PS.DISPLAY).

Umgesetzte SFR		
FMT_SMR.1/NK	FMT_MTD.1/NK	FMT_SMF.1/NK
FIA_UID.1/NK.SMR	FTP_TRP.1/NK.Admin	

Administratoren müssen sich authentisieren, bevor sie die Konfigurationsdienste des TOE verwenden können.

Die lokale Administration ist aus dem LAN des Leistungserbringers über die Schnittstelle LS.LAN.HTTP_MGMT erreichbar. Zu diesem Zweck verfügt der TOE über einen TLS-Server, der einseitige Authentisierung des Servers vorsieht. Nach dem Aufbau der TLS-Verbindung muss der Benutzer sich gegenüber der Web-Anwendung mit Benutzername und Passwort als Administrator authentisieren. Bei dieser Verbindung ist der TOE Server, der Browser des Administrators ist Client. Der TLS-Server des TOE unterstützt TLS 1.2.

Umgesetzte SFR	
FMT_SMR.1/NK	FIA_UID.1/NK.SMR
FMT_MSA.4/NK	FTP_TRP.1/NK.Admin

Alle Aktionen, die über die Management-Anwendung durchgeführt werden (login, logout, Konfigurationsänderungen) werden im Sicherheitsprotokoll gespeichert.

Diese Sicherheitsfunktion bietet eine Komponente, mit der die Firmware der KoCoBox MED+ – inklusive dem Bootloader – sicher aktualisiert werden kann. Mit Hilfe dieser Funktion werden alle Komponenten des Konnektors aktualisiert: sowohl der Netz- als auch der Anwendungskonnektor. Allerdings beschränkt sich die Sicherheitsfunktion auf das Prüfen und Aktualisieren der Firmware. Der Import der Firmware (Upload über die Management-Anwendung oder Download vom KSR-Server) wird nicht vom Netzkonnektor erbracht, sondern von Teilen des Anwendungskonnektors.

7.1.7. Kryptografische Dienste/NK (SF.CryptographicServices/NK)

Die Sicherheitsfunktion SF.CryptographicServices/NK stellt Implementierungen verschiedener kryptographischer Basisalgorithmen zur Verfügung, die von anderen Sicherheitsfunktionen des Konnektors verwendet werden können.

Zufallszahlen

Der TOE enthält einen DRNG nach FCS_RNG.1/Hash_DRBG, um Zufallszahlen hoher Qualität zu erzeugen. Der nach [NIST SP 800-90A] umgesetzte DRNG wird in regelmäßigen Abständen (alle 2.048 Zugriffe) mit 32 Bytes aus dem Zufallsgenerator der gSMC-K#2 initialisiert. Die so erzeugten Zufallszahlen werden für verschiedene Zwecke verwendet, u.a. beim TLS-Verbindungsaufbau (FCS_CKM.1/NK.TLS und FCS_COP.1/NK.TLS.AES)

Umgesetzte SFR
FCS_RNG.1/Hash_DRBG

Hash-Algorithmen

Die Funktion bietet Implementierungen für die Hash-Algorithmen SHA-1, SHA-256 und SHA-512. Im Kontext von TLS implementiert der TOE außerdem SHA-384 für bestimmte Cipher Suites.

Umgesetzte SFR
FCS_COP.1/NK.Hash, FCS_CKM.1/NK.TLS

HMAC Generierung

Die Funktion bietet darüber hinaus Algorithmen für die HMAC-Generierung, wobei die genannten Hash-Algorithmen zum Tragen kommen: HMAC-SHA-1(-96), HMAC-SHA-256(-128).

Umgesetzte SFR
FCS_COP.1/NK.HMAC, FCS_COP.1/NK.TLS.HMAC

Signaturverifikation

Die Sicherheitsfunktion SF.CryptographicServices/NK bietet Algorithmen zur Verifikation von Signaturen. X.509-Zertifikate werden unter Verwendung des RSA-PKCS1-v1.5- bzw RSASSA-PSS-Algorithmus geprüft. Zur Verifikation der Signatur der BNetzA-VL muss aktuell noch das Schema RSA-PKCS1-v1.5 verwendet werden. Das Schema RSASSA-PSS wird auch zur Verifikation von Signaturen der Software Updates, der TSL und der CRL verwendet. Zusätzlich werden damit die Hashes des sicheren Datenspeichers und die Integrität der TSF geprüft. Die Hashes des sicheren Datenspeichers wird nicht vom TOE signiert, sondern von der gSMC-K in der Betriebsumgebung des Konnektors. Die Generierung von Hashes und Zufallszahlen wird vom TOE durchgeführt.

Umgesetzte SFR
FCS_COP.1.1/NK.Auth

IPsec

Der TOE setzt das IPsec Protokoll um und verifiziert beim IKEv2 Schlüsselaustausch die Signaturen für die Authentisierung von VPN-Konzentratoren.

Dabei wird RSA PKCS#1 1.5 verwendet. Während des Schlüsselaustausches wird mit dem Diffie-Hellman Verfahren ein gemeinsames Geheimnis etabliert [RFC 7296]. Auf der Basis des ausgehandelten Geheimnisses wird mit PRF-HMAC-SHA-256 Schlüsselmaterial für den Integritätsschutz und Verschlüsselung während IKE und ESP generiert [RFC 7296, Abschnitt 2.14]. Der VPN-Verkehr wird mit ESP und den zuvor generierten Schlüsseln verschlüsselt. Die Integrität des VPN-Verkehrs wird über die Berechnung von HMACs mit dediziert generierten Schlüsseln sichergestellt. Schlüssel, die nicht mehr verwendet werden, werden durch das Überschreiben mit einer Konstanten sicher gelöscht.

Umgesetzte SFR		
FCS_COP.1/NK.IPsec	FCS_COP.1/NK.Auth	FCS_COP.1/NK.ESP
FCS_CKM.2/NK.IKE	FCS_CKM.1/NK	FCS_CKM.4/NK
FCS_COP.1/NK.HMAC		

AES / Sicherer Datenspeicher

Der TOE legt seine Logdateien und den sicheren Datenspeicher im persistenten Speicher ab. Sowohl die Logdateien als auch der sichere Datenspeicher liegen auf Dateisystemen, die mit AES im CBC Modus und 256 Bit langen Schlüsseln verschlüsselt sind. Um unvorhersagbare Initialisierungsvektoren für CBC zu erlangen, wird das Encrypted Salt-Sector IV (ESSIV) Verfahren verwendet. Die AES-Schlüssel werden beim initialien Start des TOE von der gSMC-K#1 generiert und in dieser abgelegt.

Die Erzeugung der Schlüssel wird von der gSMC-K umgesetzt. Die Schlüssel werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt.

Umgesetzte SFR	
FCS_COP.1/Storage.AES	FCS_CKM.4/NK

TLS

Der TOE stellt die Umsetzung des TLS-Protokolls in der Version 1.2 bereit. Dabei kann der TOE sowohl Client als auch Server sein. Die Funktion stellt die Integrität und Vertraulichkeit der Verbindungen zu anderen vertrauenswürdigen IT-Systemen, aber auch zum Web-Browswer des Administrators sicher. Der Netzkonnektor stellt die technischen Grundlagen für TLS bereit. Die genaue Verwendung der TLS-Verbindungen und eine Auflistung der Kommunikationspartner befindet sich in Tabelle B.4 auf Seite 149. Der Anwendungskonnektor ist dafür verantwortlich, die TLS-Verbindungen so zu konfigurieren, dass die zweckangemessen parametrisiert sind.

Umgesetzte SFR
FCS_CKM.1/NK.TLS
FMT_MOF.1/NK.TLS

Für die Generierung von Nonces und Schlüsseln verwendet der TOE den Hash_DRBG Zufallsgenerator nach FCS_RNG.1/Hash_DRBG [NIST SP 800-90A], der durch die gSMC-K#2 geseedet wird. Session Keys werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt.

Umgesetzte SFR		
FCS_CKM.1/NK.TLS		
FCS_CKM.4/NK	FCS_COP.1/NK.TLS.HMAC	FCS_COP.1/NK.TLS.AES
FCS_COP.1/NK.TLS.Auth		

JSSE erlaubt die Wiederaufnahme bestehender Sessions. Durch eine Anpassung an der JRE wurde die maximale Zeitspanne für eine Wiederaufnahme auf 24 Stunden begrenzt. Die JRE beherrscht von sich aus die session renegotiation nach [RFC 5746].

Die weiteren SFR aus Abschnitt 6.2.8 werden nicht von JSSE umgesetzt. Im Fall einer zertifikatsbasierten Authentisierung kann der TOE X.509 Zertifikate importieren oder selbst erzeugen und an den Benutzer ausliefern.

Umgesetzte SFR		
FDP_ITC.2/NK.TLS	FCS_CKM.1/NK.Zert	FPT_TDC.1/NK.TLS.Zert
FDP_ETC.2/NK.TLS		

7.2. TOE Sicherheitsfunktionen des Konnektors

7.2.1. Kryptografische Dienste/AK (SF.CryptographicServices/AK)

Die Sicherheitsanforderung FCS_COP.1/AK.SHA fordert die Umsetzung sicherer Hash-Algorithmen. Der TOE bietet Funktionen zur Berechnung von Hashwerten nach den Algorithmen SHA-256, SHA-512/256, SHA-384 und SHA-512.

Umgesetzte SFR
FCS_COP.1/AK.SHA

Die Sicherheitsfunktionalität ist ebenfalls dafür zuständig, die AES-Schlüssel für den Verschlüsselungsdienst und die Administrationsfunktionen des TOE (für den Export der Konfiguration) zu erstellen. Die Zufallszahlen, die hierfür benötigt werden, stammen von SF.CryptographicServices/NK.

Umgesetzte SFR	
FCS_CKM.4/AK	FCS_CKM.1/AK.AES

7.2.2. TLS Protokoll (SF.TLS)

Der TOE nutzt TLS zur Kommunikation mit anderen IT-Systemen sowohl in der Telematikinfrastruktur, im Internet als auch im LAN des Leistungserbringers. Tabelle B.4 zeigt die TLS-Verbindungen der KoCoBox MED+.

Die Sicherheitsanforderungen an verschiedene Verbindungen des TOE mit anderen IT-Produkten werden durch die Sicherheitsfunktion SF.TLS umgesetzt. Bei diesen Sicherheitsanforderungen geht es primär um die logische Separation der Verbindung von anderen Kommunikationskanälen, sowie die Forderung von Integrität und Authentizität der Verbindung. Die Sicherheitsfunktion regelt auch, mit welchem Zertifikat sich der TOE gegenüber den Kommunikationspartnern authentisiert.

Umgesetzte SFR		
FDP_ACC.1/AK.TLS	FDP_ACF.1/AK.TLS	FDP_UIT.1/AK.TLS
FDP_UCT.1/AK.TLS	FTP_ITC.1/AK.VZD	FTP_ITC.1/AK.eHKT
FTP_ITC.1/AK.CS	FTP_ITC.1/AK.FD	FTP_ITC.1/AK.KSR
FTP_ITC.1/AK.TSL	FIA_API.1/AK.TLS	

Das TLS Protokoll wird im TOE von den Java Secure Socket Extension (JSSE) implementiert, das Teil der Java-Laufzeitumgebung ist. JSSE wird durch Konfigurationsvorgaben und eigene Anpassungen so gehärtet, dass die Anforderungen des Schutzprofils umgesetzt werden. Die kryptographischen Eigenschaften der TLS Verbindungen werden durch die Sicherheitsfunktion SF.CryptographicServices/NK des Netzkonnektor festgelegt und umgesetzt.

Die AK-TLS-SFP sieht in ihrer Sicherheitsanforderung FDP_ACF.1/AK.TLS an verschiedenen Stellen einen TLSConnectionIdentifier vor, auf den Bezug genommen werden muss, um eine TLS Verbindung nutzen zu können. Dieser TLSConnectionIdentifier manifestiert sich nicht in der vorliegenden Implementierung. Das Framework JSSE exponiert einen solchen Identifier nicht, sondern sorgt mit Hilfe von Objekt-Referenzen und Socket-Abstraktionen für die Separation der TLS-Verbindungen des Konnektors.

7.2.3. Authentisierung (SF.Authentication)

Zusätzlich zur Authentisierung mit kryptographischen Zertifikaten ist der TOE in der Lage, Authentisierungen anhand von Passwörtern oder zuvor ausgehandelten Geheimnissen (preshared secrets) durchzuführen. Die Sicherheitsanforderung FIA_UAU.5/AK formuliert die Authentisierungsverfahren für Administratoren, Clientsysteme, Smart Cards und für eHealth-Kartenterminals.

Management-Schnittstelle

Für die Authentisierung von Administratoren an der Management-Schnittstelle der KoCoBox MED+ werden Passwörter verwendet, die über die Management-Schnittstelle vergeben werden. Diese Passwörter unterliegen Beschränkungen, die in FIA_SOS.1/AK.Passwörter formuliert sind. Passwörter werden im TOE verschlüsselt abgespeichert. Wenn bei der Authentisierung eine ungültige Kombination aus Benutzernamen und Passwort eingegeben wird, erzwingt der TOE eine dreisekündige Pause vor der nächsten Eingabemöglichkeit. Diese Zwangspause erstreckt sich nicht auf eine Netzwerkverbindung, sondern auf den übermittelten Benutzernamen.

Clientsysteme

Abhängig von der Konfiguration des Konnektors kann sich ein Clientsytem anhand eines X.509 Zertifikats oder anhand eines Passworts authentisieren (FMT_MSA.1/AK.TLS, FMT_MSA.3/AK.TLS). Die Regeln für die Passwörter für Clientsysteme sind in FIA_SOS.1/AK.CS.Passwörter beschrieben. Hierbei ist besonders ST-Anwendungshinweis 14 zu beachten. Administratoren können Zertifikate für Clientsysteme entweder importieren oder vom Konnektor erzeugen lassen. Erzeugte Zertifikate werden in einem passwortgeschützten PKCS12-Container ausgeliefert.

Kartenterminals

Die Authentisierung von eHealth-Kartenterminals erfolgt in zwei Stufen: Zuerst wird das Kartenterminal im Rahmen des TLS-Handshakes anhand eines X.509 Zertifikats authentisiert, das von der SMC-KT des eHealth-Kartenterminals stammt[1]. In der zweiten Stufe wird ein Challenge-Response basiertes Verfahren verwendet. Der Konnektor sendet das Kommando EHEALTH TERMINAL AUTHENTICATE an das Kartenterminal (FIA_SOS.2/AK.PairG).

Kartenbasierte Authentisierung

Im Kontext der Smart Card basierten Operationen ist es notwendig, dass der Konnektor die gegenseitige Authentisierung von Smart Cards ermöglicht. Dieses Verfahren wird Card to Card (C2C) Authentisierung genannt. Der Konnektor unterstützt drei Varianten dieses Verfahrens: einseitige Authentisierung, gegenseitige Authentisierung und gegenseitige Authentisierung mit Ableitung eines kryptographischen Schlüssels (FIA_UAU.5/AK und FIA_API.1/AK).

[1] Die Formulierung in FIA_UAU.5/AK kann missverstanden werden, dass das Pairing-Geheimnis in die Authentisierung des TLS-Kanals eingeht. Dort kommen aber ausschließlich X.509 Zertifikate zum Einsatz, vgl. ST-Anwendungshinweis 15.

Bei Stapelsignaturen muss sich der TOE gegenüber der QSEE (also dem HBAx) authentisieren; dazu wird das Card2Card-Verfahren angewendet. Der Konnektor weist sich gegenüber dem HBAx mit der gSMC-K#3 aus. aufgerufen. Die zur Authentisierung verwendete gSMC-K ist nicht konfigurierbar, der Ablauf der Authentisierung selbst wird von den beiden Karten bestimmt, sodass der TOE keinen Einfluss darauf hat.

Der TOE unterstützt die einseitige und gegenseitige asymmetrische Authentisierung von Chipkarten (Card2Card), die gegenseitige Authentisierung auch mit Ableitung eines symmetrischen Schlüssels und Etablierung eines sicheren Kommunikationskanals (Trusted Channel). Weiterhin unterstützt der TOE die gegenseitige symmetrische Authentisierung mit einer Chipkarte einschließlich Aushandlung symmetrischer Schlüssel für einen Secure Messaging Kanal. Die Implementierung des Card2Card Mechanismus bildet streng die Spezifikationslage ab, wie in TUC_KON_005 [gemSpec_Kon] beschrieben. Die Funktionalität wird im Rahmen unterschiedlicher UseCases genutzt, eine detaillierte Auflistung hierzu findet sich ebenfalls in TUC_KON_005.

Die Funktionalität zur Erstellung einer qualifizierten Signatur wird durch den Signaturdienst über eine definierte Schnittstelle zur Verfügung gestellt. Wird die Erstellung einer qualifizierten Signatur über diese Schnittstelle angestoßen, prüft die Anwendungslogik die relevante Konfiguration und Parametrisierung daraufhin, ob die Nutzung eines sicheren Kanals zwischen TOE (gSMC-K#3) und HBA (QSEE) notwendig ist. Wenn es sich um einen HBA als Signaturerstellungseinheit handelt und außerdem entweder das SecurityEnvironment SE_2 gesetzt ist oder es sich um eine Stapelsignatur handelt, wird der Aufbau des sicheren Kanals (C2C MUTUAL+TC) angestoßen.

Nur wenn der Kanal sicher aufgebaut werden konnte, wird die Signaturerstellung fortgesetzt. Kommt es zu Fehlern beim Aufbau des sicheren Kanals, wird die Signaturerstellung abgebrochen und eine Exception erzeugt, die im weiteren Workflow in einen SOAPFault umgewandelt wird.

In einem CV-Zertifikat einer Chipkarte ist das Zugriffsprofil dieser Chipkarte enthalten. Bei der gegenseitigen Authentisierung von Chipkarten wird dieses Zugriffsprofil ausgewertet.

Die KoCoBox MED+ führt beim Systemstart automatisierte Prozesse durch, bspw. den Selbsttest. Dies erfordert, dass bestimmte Aktionen bereits zugelassen sind, bevor ein Benutzer authentisiert ist. Solche Aktionen werden zu einem späteren Zeitpunkt wieder eingeschränkt (FIA_UID.1/AK, FIA_UAU.1/AK).

Umgesetzte SFR		
FIA_UAU.1/AK	FIA_UID.1/AK	FIA_SOS.2/AK.PairG
FIA_UAU.5/AK	FIA_API.1/AK	FIA_SOS.1/AK.Passwörter
FMT_MSA.1/AK.TLS	FMT_MSA.3/AK.TLS	FIA_SOS.1/AK.CS.Passwörter

7.2.4. Zugriffssteuerung (SF.AccessControl)

Eingehende Requests von Clientsytemen werden vom TOE anhand eines Regelwerks zugelassen oder abgelehnt. Die Datengrundlage für dieses Regelwerk ist das Informationsmodell des Konnektors. Ein eingehender Request enthält die IDs des Mandanten, des Clientsystems und des Arbeitsplatzes, von dem aus der Request generiert wurde. Diese Angaben bilden den Kontext des Requests. Das Informationsmodell definiert die Ressourcen, die vom Konnektor verwaltet werden. Es enthält transiente und persistente Objekte, aber auch Beschreibungen der Relationen zwischen dieses Objekten. Das Regelwerk, das auf Basis der Daten des Informationsmodells die Zugriffe erlaubt, nutzt die Daten des Kontexts des Requests als Eingangsdaten für die Regeln (FDP_ACC.1/AK.Infomod und FDP_ACF.1/AK.Infomod).

Die transienten Objekte des Informationsmodells werden erzeugt, wenn dem Konnektor Ressourcen zugeordnet werden. Solche Objekte werden automatisch wieder gelöscht, wenn die Ressourcen entfernt werden. Die persistenten Objekte des Informationsmodells hingegen werden von einem Benutzer mit der Rolle Administrator verwaltet (FMT_MSA.1/AK.Infomod). Default-Werte (Standardvorgaben) existieren im Informationsmodell des Konnektors nicht. Somit kann ein Administrator auch keine abweichenden Default-Werte spezifizieren (FMT_MSA.3/AK.Infomod).

Die Sicherheitsfunktionalität SF.AccessControl setzt den TUC_KON_000 („Prüfe Zugriffsberechtigung“) um.

Umgesetzte SFR	
FDP_ACC.1/AK.Infomod	FDP_ACF.1/AK.Infomod
FMT_MSA.1/AK.Infomod	FMT_MSA.3/AK.Infomod

7.2.5. Management der eHealth-Kartenterminals (SF.CardTerminalMgmt)

Der Kartenterminaldienst des TOE folgt den Spezifikationen der gematik in [gemSpec_Kon]. Seine Aufgabe ist es, die Kartenterminals und die Verbindungen zu den Kartenterminals zu managen. Ein dem Konnektor bekanntes Kartenterminal befindet sich aus Sicht des Konnektors ein einem von vier Zuständen: *bekannt*, *zugewiesen*, *gepairt* und *aktiv*. Im Zustand *aktiv* gibt es zwei Varianten: Das Kartenterminal ist entweder *verbunden* oder nicht. Ein Kartenterminal kann vom Konnektor nur in technischen Use Cases (TUC) verwendet werden, wenn es im Zustand *aktiv/verbunden* ist.

Den Clientsystemen und internen Benutzern stellt der Kartenterminaldienst Funktionen zur Interaktion mit dem Kartenterminal zur Verfügung:

- Anfordern einer Karte
- Auswerfen einer Karte

Dies sind die einzig möglichen Interaktionen von außen. Interne Benutzer können darüber hinaus eine weitere Funktion nutzen:

- Darstellen von Texten auf dem Display des Kartenterminals

Die Funktionalitäten des Kartenterminaldienstes und des Kartendienstes (zur Kommunikation mit den Karten selbst, in Abgrenzung zur Kommunikation mit den Kartenterminals) bilden ein gemeinsames logisches Subsystem. Ausschließlich dieses Subsystem sendet APDUs an Karten oder Kartenterminals, wodurch die Vorgaben der Anforderungen FDP_ACC.1/AK.eHKT und FDP_ACF.1/AK.eHKT umgesetzt werden.

Die Kommunikation mit den Kartenterminals erfordert stets eine gegenseitig authentisierte TLS-Verbindung, die gemäß den Sicherheitsattributen in SF.TLS konfiguriert ist (FDP_UCT.1/AK.TLS, FDP_UIT.1/AK.TLS, FTP_ITC.1/AK.eHKT und FPT_TEE.1/AK).

Diejenigen Attribute der Kartenterminals, die dem TOE bekannt sind, stellen einen Teil der Konfigurationsdaten des Konnektors dar und können folglich nur von einem Benutzer mit der Rolle Administrator administriert und exportiert werden (FMT_MTD.1/AK.eHKT_Abf, FMT_MTD.1/AK.eHKT_Mod).

Ein Kartenterminal ist im Konnektor unter seinem SICCT-Terminalnamen bekannt. Der Name wird in der Spezifikation auch als *FriendlyName* bezeichnet. Für den *FriendlyName* gelten Einschränkungen in Bezug auf die Länge und den Zeichensatz: Er darf zwischen 1 und 32 Zeichen lang sein und Zeichen

aus der Menge a-z, A-Z, 0-9 sowie den Bindestrich „-“ enthalten. Kartenterminals, die bei einem Broadcast gefunden werden und deren Name nicht diesen Vorgaben entspricht, werden nicht angezeigt und können nicht gepairt werden. Wenn bestehende Kartenterminals ungültige Zeichen im Namen haben, werden diese Kartenterminals nach Aktualisierung gelöscht und anschließend über den *CT/ERROR 20080* im Sicherheitsprotokoll protokolliert.

Umgesetzte SFR		
FDP_ACC.1/AK.eHKT	FDP_ACF.1/AK.eHKT	FTP_ITC.1/AK.eHKT
FDP_UCT.1/AK.TLS	FDP_UIT.1/AK.TLS	FPT_TEE.1/AK
FMT_MTD.1/AK.eHKT_Abf	FMT_MTD.1/AK.eHKT_Mod	

7.2.6. Management der Smart Cards (SF.SmartCardMgmt)

Die unter SF.SmartCardMgmt zusammengefassten Sicherheitsfunktionen beschreiben die Verfahren zum Umgang des Konnektors mit Smart Cards der Typen HBA, SMC-B, eGK und KVK, die in ein vom Konnektor kontrolliertes e-Health Kartenterminal eingesteckt werden.

Wenn eine Smart Card in ein solches Kartenterminal eingesteckt wird, werden Typ und Version der Karte identifiziert. Wenn die Karte keinem der bekannten Typen entspricht, wird sie als *unbekannt* markiert und kann nicht für weitere Operationen verwendet werden. Gehört die Karte zu einem der bekannten Typen, erstellt der Kartendienst ein Objekt für diese Karte und weist diesem ein Kartenhandle zu, sodass die Karte referenziert werden kann. Das Kartenhandle ist solange gültig, bis die Karte aus dem Kartenterminal herausgezogen wird. Andere Dienste des Konnektors können die Karte verwenden. Externen Entitäten wie Clientsytemen und Fachdiensten dürfen die Karte nur eingeschränkt verwenden. „Verwenden“ bedeutet hier, dass die Karte über den Kartendienst referenziert werden kann. Der direkte Zugriff auf die Karte und das Versenden von Kartenkommandos ist dem Kartendienst vorbehalten, vgl. Abschnitt 7.2.5.

Kartenbasierte Operationen werden im Kontext von Kartensitzungen (card session) ausgeführt. Diese Kartensitzungen werden vom Konnektor kontrolliert und laufen isoliert voneinander. Die Sicherheitszustände der Karten sind an Kartensitzungen gekoppelt und somit streng separiert. Der Sicherheitszustand einer Kartensitzung kann durch Interaktion mit dem Benutzer (durch Eingabe einer PIN) oder durch Card-to-Card-Authentisierung verändert werden.

Bei einer PIN-Authentisierung gibt der Benutzer seine PIN am Kartenterminal ein, in dem Karte steckt. Es ist auch möglich, die PIN an einem entfernten Kartenterminal einzugeben, wenn dieses entsprechend konfiguriert ist. In diesem Fall sorgt der Konnektor für den Aufbau eines sicheren Kanals (secure messaging channel), der durch das kryptographische Material der beteiligten Karten abgesichert wird.

Bei einer Card-to-card-Authentisierung steuert der Konnektor den Prozess, in dem eine Smart Card sich gegenüber einer anderen Karte im Rahmen eines challenge-response Verfahrens authentisiert. Auch hier wird kryptographisches Material verwendet, das sicher auf den Karten abgelegt sind – in diesem Fall die card verification certificates (CVC).

Die privaten Schlüssel der vom Konnektor kontrollierten Smart Cards werden für digitale Signaturen und Entschlüsselung verwendet. Darüber hinaus bieten die Karten noch begrenzten Speicherplatz für Benutzerdaten.

Die vorliegende Implementierung weicht architekturell von den Subjekten ab, die im Schutzprofil definiert werden. Die Sicherheitsanforderung FDP_ACF.1.2/AK.KD macht präzise Aussagen, welche Teile des TOE welche Aufgaben in Bezug auf Chipkarten haben. Die KoCoBox MED+ ist so aufgebaut,

dass *ausschließlich* der Kartendienst Chipkartenkommandos an die Karte absetzt. In Abgrenzung dazu kommunizieren weder der Verschlüsselungs- noch der Signaturdienst mit der Karte. Dies ist zu berücksichtigen, wenn die Architektur bewertet wird.

Umgesetzte SFR		
FDP_ACC.1/AK.KD	FDP_ACC.1/AK.PIN	FPT_TEE.1/AK
FDP_ACF.1/AK.KD	FDP_ACF.1/AK.PIN	FMT_MSA.4/AK
FMT_MTD.1/AK.Zert		

7.2.7. Signaturdienst (SF.SignatureService)

Der TOE enthält eine Signaturerstellungs- und Verifikationsanwendung (SCaVA). Diese Funktionen werden vom Signaturdienst bereitgestellt und stehen internen Benutzern und den Clientsytemen zur Verfügung. Die SCaVA kann sowohl qualifizierte als auch nicht-qualifizierte elektronische Signaturen erstellen und verifizieren. Die unterstützten Dateiformate sind:

Für nonQES PDF/A, Text, TIFF und Binärdaten

Für QES XML, PDF/A, Text, TIFF

Die Konnektorspezifikation definiert in den übergreifenden Festlegungen die Begriffe *nonQES_DocFormate* und *QES_DocFormate* um die Dateiformate zu referenzieren. Der Signaturdienst des TOE unterstützt bei der Verifkation von Signaturen verschiedene Verfahren:

- PKCS#1 RSASSA-PSS
- PKCS#1 RSASSA-PKCS1-v1_5
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Die Sicherheitsfunktion SF.SignatureService erfüllt die Anforderungen, die durch die SFR aus der Familie FCS_COP aufgestellt werden.

Umgesetzte SFR		
FCS_COP.1/AK.XML.Sign	FCS_COP.1/AK.CMS.Sign	FCS_COP.1/AK.PDF.Sign
FCS_COP.1/AK.XML.SigPr	FCS_COP.1/AK.CMS.SigPr	FCS_COP.1/AK.PDF.SigPr
FCS_COP.1/AK.PKCS.SigPr	FCS_COP.1/AK.SigVer.SSA	FCS_COP.1/AK.SigVer.PSS
FCS_COP.1/AK.SigVer.ECDSA		

Die Nutzung des Signaturdienstes wird durch SFR gesteuert, die in den Signaturerstellung-SFP und Signature Verification-SFP des Schutzprofils definiert werden. Nicht nur die Nutzung des Signaturdienstes, sondern auch die inneren Abläufe unterliegen den SFR.

Umgesetzte SFR		
FDP_ACC.1/AK.Sgen	FDP_ACC.1/AK.SigPr	FDP_ITC.2/AK.Sig
FDP_ACF.1/AK.Sgen	FDP_ACF.1/AK.SigPr	FMT_MSA.3/AK.Sig

Signaturen werden von den beteiligten Smart Cards erzeugt, die unter der Kontrolle des Kartendienstes stehen. Der Signaturdienst verhält sich unterschiedlich, je nachdem ob qualifizierte oder nichtqualifizierte Signaturen verarbeitet werden sollen. Wenn ein Dokumentenstapel mit einer qualifizierten Signatur versehen wird, sind besondere Maßnahmen erforderlich. FIA_UAU.5.2/AK(4) fordert, dass die TSF den HBA authentisieren:

Als QSEE wird der HBA authentisiert, wenn beim Stecken der Karte der richtige Typ gemäß [gemSpec_COS] und [gemSpec_HBA_ObjSys] vorhanden ist. Das CardHandle wird als Merkmal verwendet, um die Karte später zu identifizieren und mit einem Signatur-Request zu assoziieren.

Als Empfänger der DTBS und der PIN wird der HBA authentisiert, wenn beim Card2Card Schlüssel ausgehandelt werden.

Fortlaufend während des Signaturprozesses wird der HBA authentisiert durch den Aufbau eines Trusted Channel zwischen der gSMC-K#3 und dem HBA.

Umgesetzte SFR	
FTP_ITC.1/AK.QSEE	FIA_UAU.5.2/AK

Wenn eine qualifizierte Signatur erstellt wird, wird der Benutzer durch die Eingabe der PIN.QES der HBAx Smart Card authentisiert. Diese Eingabe kann entweder an dem lokalen Kartenterminal erfolgen, in dem auch der HBAx gesteckt ist, oder aber an einem entfernten Kartenterminal (über das Remote PIN Verfahren). In diesem Fall steckt der HBAx in einem zentralen Kartenterminal, das nicht am Arbeitsplatz des Benutzers steht. Der Benutzer gibt die PIN am Kartenterminal seines Arbeitsplatzes ein (das als remote Kartenterminal konfiguriert sein muss). Es besteht eine sichere Verbindung (secure messaging) zwischen dem Kartenterminal am Arbeitsplatz und dem Kartenterminal, das den HBAx enthält. Der Benutzer kann anhand der Jobnummer, die auf dem Display des Kartenterminals an seinem Arbeitsplatz angezeigt wird, feststellen, ob die PIN für den von ihm initiierten Signaturvorgang abgefragt wird.

Umgesetzte SFR	
FTA_TAB.1/AK.Jobnummer	FMT_MSA.4/AK
FIA_SOS.2/AK.Jobnummer	FTA_TAB.1/AK.SP

Der Benutzer des TOE soll der Authentizität der Signaturen (für QES und nonQES) und Zertifikate versichert sein. Die Sicherheitsfunktion SF.SignatureService stellt die Nachweise bereit, um diese Versicherung zu gewährleisten. Diese Nachweise stehen in Form von Verification Reports zur Verfügung, wie sie von der Konnektorspezifikation in TAB_KON_066 gefordert und profiliert werden [gemSpec_Kon, Abschnitt 4.1.8.5.2].

Dokumente und zu signierende Daten (DTBS) werden niemals permanent im TOE gespeichert, sodass eine Überwachung der DTBS zur Sicherstellung der Integrität in der vorliegenden Architektur nicht umgesetzt ist. Die Integrität der zu signierenden Daten, die von FDP_SDI.2/AK gefordert wird, setzt der TOE um, indem die von der Karte berechnete Signatur gegen den Hashwert der zu signierenden Daten geprüft wird.

Umgesetzte SFR	
FDP_DAU.2/AK.Cert	FDP_SDI.2/AK

Signaturrichtlinien

Eine besondere Bedeutung kommt im Kontext des Signaturdienstes den *Signaturrichtlinien* zu. Diese Richtlinien profilieren das Signieren von Dokumenten und das Verifizieren von Signaturen. Leider ist der Begriff „Signaturrichtlinie“ im Kontext des Konnektors nicht eindeutig gefasst. Schutzprofil und Konnektorspezifikation interpretieren den Begriff unterschiedlich. Im Folgenden werden die Interpretationen beschrieben und die für dieses Dokument angenommene Interpretation dargelegt.

Schutzprofil Das Schutzprofil interpretiert „Signaturrichtlinie“ bewusst weit. Im Glossar in [BSI-CC-PP-0098] wird der Begriff als „Profilierung der Signaturformate“ definiert. Er dient z. B. zur Unterscheidung zwischen qualifizierten und nicht-qualifizierten Signaturen. FDP_DAU.2.1/AK.QES und FDP_DAU.2.1/AK.Sig listen die vom Konnektor zu unterstützenden Dokumentformate, Signaturformate und Signaturvarianten auf; sie machen jedoch keine Aussagen darüber, welche Elemente technisch und fachlich sinnvoll verknüpfbar sind.

Darüber hinaus führt das Glossar noch die *zulässige Signaturrichtlinie* auf, die u. a. auf die Anwendbarkeit der zu signierenden Daten durch den EVG abstellt. Dies kann als Einschränkung der Kombinationsmöglichkeiten aus FDP_DAU.2.1/AK.QES verstanden werden. Gestützt wird diese Annahme durch die Anforderung aus FMT_MSA.1.1/AK.User(2)[2], die die Auswahl der Signaturrichtlinie den Benutzern des Clientsystems vorbehält.

Konnektorspezifikation Die Konnektorspezifikation interpretiert „Signaturrichtlinie“ enger als das Schutzprofil. Signaturrichtlinien im Sinne der Spezifikation profilieren die Signaturerstellung und -prüfung. Sie werden über eine URI referenziert. Der Konnektor selbst stellt keine Signaturrichtlinie zur Verfügung, es obliegt den Fachmodulen, eigene Richtlinien zu definieren [gemSpec_Kon, Abschnitt 4.1.8.1.2]. Das ist das Vorgehen im Fachmodul NFDM. Legt man diese Interpretation zugrunde, so gibt es in OPB 2.1 genau eine Signaturrichtlinie.

Für dieses Security Target ist es nicht zweckdienlich, sich ausschließlich einer der beiden Interpretationen zu verschreiben und die andere nicht zu beachten. Stattdessen wird in diesem Security Target eine Interpretation angenommen, die der Obermenge der Interpretationen des Schutzprofils und der Konnektorspezifikation entspricht: Wir nehmen die Auflistungen der Elemente aus FDP_DAU.2.1/AK.QES und FDP_DAU.2.1/AK.Sig an, beschränken jedoch die Kombinierbarkeit anhand der in TAB_KON_778 vorgegebenen Einsatzbereiche. Tabelle 7.1 zeigt die verschiedenen Signaturverfahren in Bezug auf die Signatureigenschaften Gegensignatur, Parallelsignatur und OCSP-Einbettung. Zusätzlich gelten Einschränkungen bei der Verwendung von Signaturverfahren:

XAdES / QES Der Konnektor unterstützt qualifizierte Signaturen auf XML-Dokumenten ausschließlich in Verbindung mit einer benannten Signaturrichtlinie. In OPB 2.1 wird die in der Firmware des TOE verankerte Signaturrichtlinie des Fachmodul NFDM [gemRL_QES_NFDM, Abschnitt 3.] berücksichtigt, andere Signaturrichtlinien für QES werden nicht akzeptiert. Mit dieser Einschränkung setzt das Security Target die Anforderung aus TIP1-A_5538 um.

Die möglichen Transformationen bei der Erzeugung und Verifikation von XAdES Signaturen wurde stark eingeschränkt. Die einzig erlaubte Transformation ist `http://www.w3.org/2006/12/xml-c14n11` (ohne Kommentare) zur Kanonisierung der

[2] Allerdings gilt diese Annahme nur, wenn man die Begriffe „*zulässige* Signaturrichtlinie“ (aus dem Glossar) und „*gültige* Signaturrichtlinie“ (aus dem SFR) synonym betrachtet (Hervorhebungen in den Zitaten durch den ST-Autor). Das Schutzprofil bleibt hier vage.

XML-Daten. Durch die Beschränkung auf *Detached* Signaturen sind keine Transformationen zum Ausschneiden der Signatur notwendig.

XAdES / nonQES Der Konnektor unterstützt keine nicht-qualifizierten Signaturen auf XML-Dokumenten.

PAdES PAdES Signaturen, die nicht das gesamte Dokument umfassen, werden als ungültig gewertet. Weiterhin werden keine Updates auf einem bereits signierten Dokument unterstützt:

- Es können keine OCSP-Responses in den Document Security Store eingebettet werden.
- Dokumentinkludierende Gegensignaturen in Form von PDF Serial Signatures werden nicht unterstützt.

Herstellerspezifische Signaturrichtlinien Fast alle ursprünglich vom Hersteller ergänzten Signaturrichtlinien sind inzwischen durch die Spezifikationen der gematik oder das Protection Profile vorgegeben. Folgende Vorgaben/Anpassungen können darüber hinaus als herstellerspezifische Signaturrichtlinien angesehen werden:

- Sichere Ermittlung des signierten Bereichs von PDF-Signaturen nach dem Algorithmus gemäß Vulnerability Report der Ruhr-Universität Bochum. Hierdurch wird eine Härtung gegen Universal Signature Forgery (USF), Incremental Saving Attack (ISA) und Signature Wrapping Attack (SWA) erreicht.
- Härtung der zur Erstellung und Prüfung von XML-Signaturen verwendeten XML-Schemas gegen Signature Wrapping Angriffe gemäß Empfehlungen in [RUB-XML].
- Härtung der XML-Verarbeitung (Schnittstellen und Parser) gemäß *OWASP*.
- Verbot mehrerer identischer ID-Attribute in einem XML-Dokument. Die Signaturerstellung und -prüfung muss mit einer Fehlermeldung abgebrochen werden, wenn ID-Attribute nicht eindeutig sind.

Folgt man dieser Interpretation, ist auch FMT_MSA.1/AK.User umzusetzen. Damit obliegt es der Verantwortung des Benutzers des Clientsystems, über eine entsprechende Auswahl im Clientsystem die für den speziellen Anwendungszweck angemessene Signaturrichtlinie auszuwählen.

Umgesetzte SFR		
FDP_DAU.2/AK.Sig	FDP_DAU.2/AK.QES	FMT_MSA.1/AK.User

External Authenticate

Der Konnektor bietet an der Außenschnittstelle die Operation *ExternalAuthenticate* an. Diese Operation signiert einen max. 512 Byte langen Binärstring, den das Clientsystem bereitstellt. Der Konnektor verwendet ausschließlich die SMC-B oder den HBA, um Signaturen für diese Operation zu erzeugen. Der Umfang der Schnittstelle ist in TIP1-A_5439 der Konnektorspezifikation definiert [gemSpec_Kon, Abschnitt 4.1.13.4.1]. Der TOE unterstützt an dieser Schnittstelle das im Schutzprofil geforderte Verfahren PKCS#1 (RSASSA-PKCS1-v1_5, RSASSA-PSS).

Umgesetzte SFR
FDP_ACF.1.2/AK.Sgen(6)

		Parallelsignatur		Gegensignatur		OCSP-Einb.		Anz. Signat.
		Erstellen	Prüfen	Erstellen	Prüfen	Erstellen	Prüfen	
nonQES	CAdES*	✓	✓	✓	✓	✓[1]	✓[2]	unbeg.
	PAdES†	.	.	.	.	.	.	1
	XAdES×	–	–	–	–	–	–	–
QES	CAdES*	✓	✓	✓	✓	✓	✓	unbeg.
	PAdES†	.	.	.	.	.	.	1
	XAdES‡	.	.	.	.	✓	✓	1

* Für Detached und Enveloping Signaturen
† Speichern der Signatur als Incremental Update
× nonQES XAdES wird vom Konnektor nicht angeboten.
‡ Für Detached Signaturen bei NFDM

[1] Nur bei der Erstellung von Gegensignaturen
[2] Nur bei der Prüfung von Parallelsignaturen bei der Erstellung von Gegensignaturen

Tabelle 7.1.: Signaturvarianten

7.2.8. Verschlüsselungsdienst (SF.EncryptionService)

Der Konnektor ver- und entschlüsselt über seinen Verschlüsselungsdienst Dokumente hybrid und symmetrisch. Dabei wird zwischen den Datenformaten XML, PDF/A, Text, Tiff und Binärdaten unterschieden. Darüber hinaus können MIME Dokumente nach S/MIME und XML Dokumente nach der W3C Recommendation „XML Encryption Syntax and Processing“ [XMLEnc] ver- und entschlüsselt werden.

Der symmetrische Teil der Verschlüsselung folgt AES/GCM mit Schlüssellängen von 128 Bit und 256 Bit. Der asymmetrische Teil unterstützt RSAOAEP mit Schlüssellänge 2048 Bit. Die Sicherheitsfunktion setzt die Anforderungen aus der Familie FCS_COP um. Die Konnektorspezifikation wurde durch den Change C_7076 in Bezug auf die Anforderungen TIP1-A_4617, GS-A_4375 und GS-A_4376 so ersetzt, dass das Verfahren RSA RSAES-PKCS1-v1_5 nur noch optional ist [gemErrata_4_Kon_PTV3]. Gemäß dieser Anpassungen unterstützt der Konnektor ausschließlich RSAOAEP.

Umgesetzte SFR		
FCS_COP.1/AK.AES	FCS_COP.1/AK.XML.Ver	FCS_COP.1/AK.XML.Ent
FCS_COP.1/AK.MIME.Ver	FCS_COP.1/AK.MIME.Ent	FCS_COP.1/AK.CMS.Ver
FCS_COP.1/AK.CMS.Ent		

Die Verwendung der Sicherheitsfunktion unterliegt Regeln, die in weiteren Anforderungen formuliert sind. Dort ist auch beschrieben, wie der TOE mit den zu verschlüsselnden und den verschlüsselten Daten umzugehen hat.

Umgesetzte SFR	
FDP_ACC.1/AK.Enc	FDP_ACF.1/AK.Enc
FDP_ITC.2/AK.Enc	FDP_ETC.2/AK.Enc

Verschlüsselungsrichtlinien

Der Verschlüsselungsdienst ist nach den Vorgaben der gematik implementiert. Korrespondierend zu den Operationen und TUCs in [gemSpec_Kon] gibt es keine expliziten oder identifizierbaren Verschlüsselungsrichtlinien. Die Vorgaben in SFRs, die auf solche Richtlinien Bezug nehmen, werden als eine Referenz auf die [gemSpec_Kon] interpretiert, um eine spezifiktionskonforme Implementierung zu gewährleisten.

Der TOE verwendet die herstellereigene Verschlüsselungsrichtlinie, dass bei **XML-Verschlüsselung** ausschließlich das Gesamtdokument verschlüsselt wird. Das Ver- und Entschlüsseln von Teilbäumen wird nicht unterstützt.

Als Empfängerzertifikate werden zugelassen:

Zum Referenzzeitpunkt (Zeitpunkt der Verschlüsselung) zeitlich gültige Zertifikate mit der *KeyUsage* keyEncipherment und deren Signatur mit einem zum Referenzzeitpunkt zulässigen Algorithmus erfolgt ist – sowie:

1. deren CA sich in der Liste der importierten CAs befindet – oder
2. deren CA in der TSL aktiv ist, das ENC-Zertifikat zum Referenzzeitpunkt nicht widerrufen war und die mindestens eine der folgenden Policies enthält:
   a) OID_EGK_ENC (1.2.276.0.76.4.68)
   b) OID_EGK_ENCV (1.2.276.0.76.4.69)
   c) OID_HBA_ENC (1.2.276.0.76.4.74)
   d) OID_SMCB_ENC (1.2.276.0.76.4.76)

Dem Betreiber des EVG bleibt es unbenommen, CAs für Zertifikate, die den Anforderungen aus b) nicht (mehr) genügen in die unter (1) genannte Liste einzutragen um die strikten Prüfungen unter (2) zu vermeiden.

7.2.9. Sicherer Speicher (SF.SecureStorage)

Der Konnektor verfügt über einen sicheren internen Datenspeicher, um Daten verschlüsselt und signiert abzulegen. Die Verschlüsselung ist symmetrisch und für den Benutzer transparent. Der symmetrische Schlüssel für diese Daten liegt im Netzkonnektor und ist nicht von außen manipulierbar. Jede Datei, die im sicheren Datenspeicher abgelegt ist, wird einzeln signiert. Beim Lesezugriff auf diese Datei wird die Signatur geprüft. Eine invalide Signatur versetzt den TOE in einen kritischen Betriebszustand, der den Funktionsumfang des Konnektors stark einschränkt.

Umgesetzte SFR	
FDP_ACC.1/AK.SDS	FDP_ACF.1/AK.SDS

Die kryptographischen Funktionen des sicheren Datenspeichers werden von der Sicherheitsfunktion SF.CryptographicServices/NK umgesetzt, vgl. Abschnitt 7.1.7, Unterabschnitt „AES / Sicherer Datenspeicher“.

7.2.10. Versichertenstammdatenmanagement (SF.VSDM)

Das Fachmodul VSDM des Konnektors liest die Versichertenstammdaten (VSD) von den elektronischen Gesundheitskarte des Patienten ein und übermittelt sie an das Praxisverwaltungssystem. Darüber hinaus können die Stammdaten auf der eGK aktualisiert werden: Der Konnektor prüft auf dem Update Flag Service der Telematikinfrastruktur, ob eine Aktualisierung für die Daten vorliegt. Ist das der Fall, vermittelt der Konnektor einen sicheren Kanal zwischen dem Versichertenstammdatendienst der TI (VSDD) und der eGK des Patienten. Wenn dieser Kanal aufgebaut ist, sind die Daten zwischen den Kommunikationspartner Ende-zu-Ende verschlüsselt. Der Konnektor leitet den verschlüsselten Datenstrom weiter, kann die Daten aber nicht selbst lesen.

Zusätzlich zur Aktualisierung der VSD kann derselbe Mechanismus verwendet werden, um das Objektsystem der eGK zu aktualisieren. Hierbei ist jedoch der Card Management Service der TI (CMS) der Kommunikationspartner der Karte, nicht der VSDD).

Der Kommunikationsablauf wird nicht von Betriebsparametern beeinflusst, die der Administrator verändern kann. Somit gibt es auch keine Standardwerte, die der Administrator mit alternativen Werten belegen kann.

Umgesetzte SFR	
FDP_ACC.1/AK.VSDM	FDP_ACF.1/AK.VSDM
FMT_MSA.3/AK.VSDM	FMT_MSA.1/AK.VSDM

7.2.11. Administration/AK (SF.Administration/AK)

Der Konnektor enthält eine Management-Schnittstelle, die von einem Administrator über eine Web-Anwendung benutzt werden kann. Ein authentisierter Benutzer mit der Rolle Administrator kann die Verwaltungsoperationen vornehmen, die in [gemSpec_Kon] definiert sind. Unter anderem können so die Konfigurationsdaten der Konnektor Services angepasst werden. Jeder Service definiert seine eigene, begrenzte Menge an Konfigurationsdaten. Der Management Service selbst definiert übergreifende Konfigurationselemente.

Die Sicherheitsfunktionalität SF.Administration/AK ist ebenfalls dafür verantwortlich, die Konfigurationsparameter der Fachmodule des Konnektors zu managen. Auch für die Konfigurationsparameter der Fachmodule wird die Managementschnittstelle des Konnektors verwendet. Die Web Application zur Administration unterstützt dies ebenfalls. Die Validierung und Prüfung der Konfigurationsparameter für ein Fachmodul erledigt allerdings nicht der Anwendungskonnektor, sondern das Fachmodul selbst. Der Anwendungskonnektor reicht die Konfigurationsparameter an das Fachmodul weiter. Das Fachmodul prüft die Parameter und ruft die TUCs an LS.FM.RMI auf, um sie dem Anwendungskonnektor zum Persistieren zurückzugeben. Die Konnektor Security Guidance erklärt den Vorgang genauer [KoCo AGD_Kon-Sec, Abschnitt 3.4.].

Über die Managementanwendung kann auch die Konfiguration des TOE sicher exportiert werden. Die Konfigurationsdaten werden dabei symmetrisch verschlüsselt.

Umgesetzte SFR		
FMT_SMR.1/AK	FMT_SMF.1/AK	FMT_MOF.1/AK
FMT_MTD.1/AK.Admin	FMT_MSA.1/AK.TLS	FMT_MSA.3/AK.TLS

Die Managementanwendung stellt Funktionen zur Administration des Gesamtkonnektors, z. B. die Downloads der Updates vom KSR-Server oder die Anpassung des Funktionsumfangs des Konnektors

zur Verfügung. Das Schutzprofil räumt die Möglichkeit ein, dass der TOE automatische Updates seiner Firmware durchführt, wenn ein Administrator die Funktion an der Management-Schnittstelle aktiviert. Die KoCoBox MED+ setzt diese Funktionalität nicht um. Das Herunterladen und Anwendungen von Update-Paketen muss vom Administrator explizit angefordert werden.

Ein Updatepaket für den Konnektor enthält die Firmware für den Basiskonnektor und die Fachmodule. Eine Aktualisierung des Basiskonnektors enthält immer auch eine Aktualisierung der Fachmodule, diese Updates sind nicht separat voneinander einspielbar. Umgekehrt gilt, dass Fachmodule immer nur im Kontext der Updates des Basiskonnektors aktualisiert werden können. Tabelle 1.6 zeigt die Versionsnummern des TOE und der Fachmodule.

Auf Anforderung des Administrators verifiziert die Update-Komponente des TOE die Integrität und Authentizität des Update Image, indem sie einen SHA-512 Hash über das Image berechnet und dessen kryptographische Signatur mittels RSASSA-PSS und des öffentlichen Signer-Zertifikats des Herstellers überprüft. Das Zertifikat selbst wird gegen ein CA-Zertifikat geprüft, das im Root-Filesystem auf dem NAND-Flash verankert ist. Darüberhinaus wird die Firmware nur dann installiert, wenn die Versionsnummer des Update-Images in einer Liste gültiger Versionsnummern – der sogenannten Firmwaregruppe – enthalten ist. Diese Liste ist Teil des TOE und wird bei jedem Update aktualisiert.

Bei einem Firmware-Update wird immer die gesamte Systempartition (inklusive dem AK und möglicher zukünftiger Teile des Konnektors) aktualisiert. Zuerst wird die neue Firmware auf die alternative Partition des Flash-Speichers (eMMC) aufgespielt. Nach dem erfolgreichen Aufspielen wird die aktualisierte Partition als aktive Partition festgelegt und der Konnektor neu gestartet. Der Konnektor startet nur dann von der aktualisierten Partition, wenn das Update erfolgreich war. So wird garantiert, dass das Gerät auf einen konsistenten und sicheren Softwarestand zurückfällt, falls die Validierung vorher fehlgeschlagen ist, oder die neue Firmware nicht aufgespielt werden konnte. Die Inhalte des sicheren Datenspeichers – besonders die Konfigurationsdaten und die Logfiles – werden vom Updateprozess nicht berührt und bleiben erhalten.

Umgesetzte SFR		
FDP_ACC.1/AK.Update	FDP_ACF.1/AK.Update	FDP_UIT.1/AK.Update

7.2.12. Selbstschutz (SF.SelfProtection/AK)

Der Konnektor verfügt über Schutzmechanismen, um sich selbst und die verarbeiteten Daten zu schützen. Die verschiedenen Mechanismen werden in diesem Abschnitt beschrieben.

Der TOE verwendet in verschiedenen Use Cases kryptographische Zertifikate und entsprechende Validierungsverfahren, Die konkreten Schritte zur Validierung eines Zertifikats hängen von der Art des Zertifikats ab. Dabei werden CVC und X.509 Zertifikate unterschiedlich behandelt. Innerhalb der X.509 Zertifikate wird zwischen qualifizierten und nicht-qualifizierten Zertifikaten unterschieden. Bei den nicht-qualifizierten Zertifikaten wiederum macht es einen Unterschied, ob ein Zertifikat aus dem Vertrauensraum der gematik oder aus dem herstellerspezifischen Vertrauensraum der KoCo PKI stammt. Somit ergeben sich vier verschiedene Kategorien von Zertifikaten. Wenn man Sonderfälle und Ausnahmen der X.509 Zertifikate für den Moment außer Betracht lässt, verläuft eine Validierung entlang folgender Linie:

Schritt 1 Prüfung der zeitlichen Gültigkeit

Schritt 2 Prüfung der mathematischen Korrektheit

Schritt 3 Prüfung des Vertrauensstatus: Zertifikate aus dem Vertrauensraum der gematik werden gegen die Trust Service List (TSL) der gematik geprüft.

Schritt 4 Zertifikate aus dem Vertrauensraum der gematik werden auf Widerruf geprüft. Im Normalfall geschieht dies online mittels OCSP. Die Zertifikate der VPN-Konzentratoren werden gegen eine Widerrufsliste (CRL) geprüft.

Der TOE überprüft ebenfalls die Signaturen der TSL und der CRL. Beide Listen werden automatisch alle 24 Stunden durch einen HTTP-Aufruf heruntergeladen und aktualisiert.

Umgesetzte SFR
FPT_TDC.1/AK

Der Betriebszustand des TOE wird während des gesamten Betriebsablaufs überwacht. Wenn ein Modul oder ein Dienst einen relevanten[3] Fehler feststellt, wird ein interner Ereignisdienst aufgerufen, um alle anderen Dienste und registrierte Nachrichtenempfänger darüber zu informieren. Die Module entscheiden nach dem Empfang einer Nachricht, ob sie ihre Ausführung unterbrechen, solange der Fehlerzustand besteht. Diese Entscheidung wird anhand der Regeln aus der Spezifikation [gemSpec_Kon, TAB_KON_504] getroffen.

Umgesetzte SFR
FPT_FLS.1/AK

Der Konnektor führt beim Systemstart einen Selbsttest durch. Der Administrator kann den Selbsttest während der Laufzeit erneut starten. Der Selbsttest findet auch alle 24 Stunden statt (vgl. das entsprechende SFR des Netzkonnektors FPT_TST.1/NK). Der ST-Anwendungshinweis dort gilt entsprechend auch für den AK. Die Prüfung bezieht sich nicht streng auf ausführbare Dateien, sondern auch alle anderen Teil der Firmware. Damit gilt der Integritätsschutz auch für die XML-Schemadateien, aus denen sich die Signaturrichtlinien zusammensetzen.

Umgesetzte SFR	
FPT_TST.1/AK.Run-time	FPT_TST.1/AK.Out-Of-Band

Das im TOE verwendete Java Runtime Environment ist speziell für die Belange des Konnektors gehärtet worden. Es wird dafür gesorgt, dass nicht mehr benötigte kryptographische Schlüssel unmittelbar nach der Verwendung sicher gelöscht werden. Dabei werden die Speicherbereiche, in den die Schlüssel lagen, mit Nullen überschrieben. Der Garbage Collector der JRE wurde so angepasst, dass keine Schattenkopien mehr im Speicher verbleiben.

Umgesetzte SFR	
FCS_CKM.4/AK	FDP_RIP.1/AK

Die kryptographische Identität des Konnektors ist auf einer gSMC-K gespeichert. Diese Smart Card erfüllt die Anforderungen des Schutzprofils [BSI-CC-PP-0082-2] und gehört zur Einsatzumgebung. Die Schutzmechanismen werden hier nicht weiter betrachtet.

[3] Die gematik Spezifikation definiert die kritischen Fehlerzustände, vgl. [gemSpec_Kon, Abschnitt 3.3, TAB_KON_503]

7.2.13. Protokollierungsdienst/AK (SF.Audit/AK)

Sicherheitsrelevante Ereignisse des Konnektors und der Fachmodule werden in einem Protokoll permanent gespeichert. Der Speicherplatz für dieses Protokoll ist mit 900 MB angemessen groß. Beim Überlauf des Protokollspeichers werden alte Protokolleinträge zyklisch überschrieben, also die ältesten Einträge zuerst. Es gibt keinen anderen Mechanismus zum Löschen oder Ändern von Protokolleinträgen. Zum Schutz der Log-Einträge geben die Konfigurationsparameter *LOG_DAYS* (für den Basiskonnektor) und *FM_<fmName>_LOG_DAYS* (für Fachmodule) an, nach wievielen Tagen Logeinträge frühestens überschrieben werden können [gemSpec_Kon, TAB_KON_609]. Die Konfigurationsparameter *LOG_LEVEL* *FM_<fmName>_LOG_LEVEL* legt die Mindest-Schwere zu protokollierender Einträge fest.

Umgesetzte SFR		
FAU_STG.4/AK	FAU_STG.1/AK	

Der TOE ist gegen Überlauf seines Protokollspeichers geschützt. Extern ausgelöste Audit-Ereignisse werden direkt abgespeichert, falls dasselbe Ereignis nicht bereits innerhalb der letzten zwei Sekunden aufgetreten ist. Trat das Ereignis bereits in den letzten zwei Sekunden auf, wird nur der Zähler erhöht. Wenn das Ereignis danach innerhalb von zwei Sekunden nicht erneut auftritt, wird es aus der Liste entfernt und beim nächsten Auftreten als ein neues Ereignis behandelt. Wenn ein Ereignis mehrfach auftritt und der Zähler mehrfach inkrementiert wird, wird das Ereignis nach 20 Sekunden (maximale Höhe des Zählers) erneut protokolliert. Die Logs werden in einer Datenbank gespeichert und automatisch verschlüsselt (vgl. SF.CryptographicServices/NK).

Wenn der Protokollspeicher des TOE zu mehr als 80% gefüllt ist, informiert der TOE den Administrator über das Display am Gehäuse des Konnektors.

Der Protokollspeicher kann nur vom zentralen Protokollierungsdienst, nicht aber von externen Entitäten, ausgelesen werden. Zum Betrachten der Protokolleinträge greift der Administrator auf Funktionen der Managementschnittstelle zurück, die die zu präsentierenden Einträge beim Protokollierungsdienst anfordert.

Umgesetzte SFR		
FAU_GEN.1/AK	FAU_SAR.1/AK	FPT_STM.1/AK

7.3. Verhältnis von SFR zu SF des Netzkonnektors

Tabelle 7.2 zeigt, in welchem Verhältnis die im Abschnitt 6.2 definierten Sicherheitsanforderungen an den Netzkonnektors zu den in Abschnitt 7.1 beschriebenen Sicherheitsfunktionen des NK stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	SF.VPN	SF.DynamicPacketFilter	SF.NetworkServices	SF.SelfProtection/NK	SF.Audit/NK	SF.Administration/NK	SF.CryptographicServices/NK
FAU_GEN.1/NK.SecLog	.	.	.	.	✓	.	.
FAU_GEN.2/NK.SecLog	.	.	.	.	✓	.	.
FCS_CKM.1/NK.TLS	.	.	.	.	.	.	✓
FCS_CKM.1/NK.Zert	.	.	.	.	.	.	✓
FCS_CKM.1/NK	.	.	.	.	.	.	✓
FCS_CKM.2/NK.IKE	.	.	.	.	.	.	✓
FCS_CKM.4/NK	.	.	.	.	.	.	✓
FCS_COP.1/NK.Auth	.	.	.	.	.	.	✓
FCS_COP.1/NK.ESP	.	.	.	.	.	.	✓
FCS_COP.1/NK.Hash	.	.	.	.	.	.	✓
FCS_COP.1/NK.HMAC	.	.	.	.	.	.	✓
FCS_COP.1/NK.IPsec	.	.	.	.	.	.	✓
FCS_COP.1/NK.TLS.AES	.	.	.	.	.	.	✓
FCS_COP.1/NK.TLS.Auth	.	.	.	.	.	.	✓
FCS_COP.1/NK.TLS.HMAC	.	.	.	.	.	.	✓
FCS_COP.1/Sign	.	.	.	.	.	.	✓
FCS_COP.1/Storage.AES	.	.	.	.	.	.	✓
FCS_RNG.1/Hash_DRBG	.	.	.	.	.	.	✓
FDP_ETC.2/NK.TLS	.	.	.	.	.	.	✓
FDP_IFC.1/NK.PF	.	✓	.	.	.	.	.
FDP_IFF.1/NK.PF	.	✓	.	.	.	.	.
FDP_ITC.2/NK.TLS	.	.	.	.	.	.	✓
FDP_RIP.1/NK	.	.	.	✓	.	.	.
FIA_UID.1/NK.SMR	.	.	.	.	.	✓	.
FMT_MOF.1/NK.TLS	.	.	.	.	.	.	✓
FMT_MSA.1/NK.PF	.	.	.	.	.	✓	.
FMT_MSA.3/NK.PF	.	✓	.	.	.	.	.
FMT_MSA.4/NK	.	.	.	.	.	✓	.
FMT_MTD.1/NK	.	.	.	.	.	✓	.
FMT_SMF.1/NK	.	.	.	.	.	✓	.
FMT_SMR.1/NK	.	.	.	.	.	✓	.
FPT_EMS.1/NK	.	.	.	✓	.	.	.

	SF.VPN	SF.DynamicPacketFilter	SF.NetworkServices	SF.SelfProtection/NK	SF.Audit/NK	SF.Administration/NK	SF.CryptographicServices/NK
FPT_STM.1/NK	.	.	✓	.	.	✓	.
FPT_TDC.1/NK.TLS.Zert	.	.	.	.	.	.	✓
FPT_TDC.1/NK.Zert	✓	.	.	.	.	.	.
FPT_TST.1/NK	.	.	.	✓	.	.	.
FTP_ITC.1/NK.TLS	.	.	.	.	.	.	✓
FTP_ITC.1/NK.VPN_SIS	✓	.	.	.	.	.	.
FTP_ITC.1/NK.VPN_TI	✓	.	.	.	.	.	.
FTP_TRP.1/NK.Admin	.	.	.	.	.	✓	.

Tabelle 7.2.: Abbildung der SFR des NK auf Sicherheitsfunktionalität

7.4. Verhältnis von SFR zu SF des Konnektors

Tabelle 7.3 zeigt, in welchem Verhältnis die im Abschnitt 6.3 definierten Sicherheitsanforderungen an den Anwendungskonnektors zu den in Abschnitt 7.2 beschriebenen Sicherheitsfunktionen des AK stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	SF.CryptographicServices/AK	SF.TLS	SF.Authentication	SF.AccessControl	SF.CardTerminalMgmt	SF.SmartCardMgmt	SF.SignatureService	SF.EncryptionService	SF.SecureStorage	SF.VSDM	SF.Administration/AK	SF.SelfProtection/AK	SF.Audit/AK
FAU_GEN.1/AK	.	.	.	.	.	.	.	.	.	.	.	.	✓
FAU_SAR.1/AK	.	.	.	.	.	.	.	.	.	.	.	.	✓
FAU_STG.1/AK	.	.	.	.	.	.	.	.	.	.	.	.	✓
FAU_STG.4/AK	.	.	.	.	.	.	.	.	.	.	.	.	✓
FCS_CKM.1/AK.AES	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_CKM.4/AK	✓	.	.	.	.	.	.	.	.	.	.	✓	.
FCS_COP.1/AK.AES	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.CMS.Ent	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.CMS.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.CMS.Sign	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.CMS.Ver	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.PDF.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.PDF.Sign	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.PKCS.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.ECDSA	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.PSS	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.SSA	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.SHA	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/AK.MIME.Ent	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.MIME.Ver	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.XML.Ent	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/AK.XML.Sign	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.XML.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FCS_COP.1/AK.XML.Ver	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ACC.1/AK.eHKT	.	.	.	.	✓	.	.	.	.	.	.	.	.
FDP_ACC.1/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ACC.1/AK.Infomod	.	.	.	✓	.	.	.	.	.	.	.	.	.
FDP_ACC.1/AK.KD	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACC.1/AK.PIN	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACC.1/AK.Sgen	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACC.1/AK.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACC.1/AK.TLS	.	✓	.	.	.	.	.	.	.	.	.	.	.

	SF.CryptographicServices/AK	SF.TLS	SF.Authentication	SF.AccessControl	SF.CardTerminalMgmt	SF.SmartCardMgmt	SF.SignatureService	SF.EncryptionService	SF.SecureStorage	SF.VSDM	SF.Administration/AK	SF.SelfProtection/AK	SF.Audit/AK
FDP_ACC.1/AK.SDS	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACC.1/AK.Update	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_ACC.1/AK.VSDM	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_ACF.1/AK.eHKT	.	.	.	.	✓	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ACF.1/AK.Infomod	.	.	.	✓	.	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.KD	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACF.1/AK.PIN	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACF.1/AK.Sgen	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACF.1/AK.SigPr	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACF.1/AK.TLS	.	✓	.	.	.	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.SDS	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACF.1/AK.Update	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_ACF.1/AK.VSDM	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_DAU.2/AK.Cert	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_DAU.2/AK.QES	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_DAU.2/AK.Sig	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ETC.2/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ITC.2/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ITC.2/AK.Sig	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_RIP.1/AK	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_SDI.2/AK	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_UCT.1/AK.TLS	.	✓	.	.	✓	.	.	.	.	.	.	.	.
FDP_UIT.1/AK.TLS	.	✓	.	.	✓	.	.	.	.	.	.	.	.
FDP_UIT.1/AK.Update	.	.	.	.	.	.	.	.	.	.	✓	.	.
FIA_API.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_API.1/AK.TLS	.	✓	.	.	.	.	.	.	.	.	.	.	.
FIA_SOS.1/AK.Passwörter	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_SOS.1/AK.CS.Passwörter	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_SOS.2/AK.Jobnummer	.	.	.	.	.	.	✓	.	.	.	.	.	.
FIA_SOS.2/AK.PairG	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_UAU.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_UAU.5/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.
FIA_UID.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.
FMT_MSA.1/AK.Infomod	.	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_MSA.1/AK.TLS	.	.	✓	.	.	.	.	.	.	.	✓	.	.
FMT_MSA.1/AK.User	.	.	.	.	.	.	✓	.	.	.	.	.	.

	SF.CryptographicServices/AK	SF.TLS	SF.Authentication	SF.AccessControl	SF.CardTerminalMgmt	SF.SmartCardMgmt	SF.SignatureService	SF.EncryptionService	SF.SecureStorage	SF.VSDM	SF.Administration/AK	SF.SelfProtection/AK	SF.Audit/AK
FMT_MSA.1/AK.VSDM	.	.	.	.	.	.	.	.	.	✓	.	.	.
FMT_MSA.3/AK.Infomod	.	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_MSA.3/AK.TLS	.	.	✓	.	.	.	.	.	.	.	✓	.	.
FMT_MSA.3/AK.Sig	.	.	.	.	.	.	✓	.	.	.	.	.	.
FMT_MSA.3/AK.VSDM	.	.	.	.	.	.	.	.	.	✓	.	.	.
FMT_MSA.4/AK	.	.	.	.	.	✓	✓	.	.	.	.	.	.
FMT_MOF.1/AK	.	.	.	.	.	.	.	.	.	.	✓	.	.
FMT_MTD.1/AK.Admin	.	.	.	.	.	.	.	.	.	.	✓	.	.
FMT_MTD.1/AK.Zert	.	.	.	.	.	.	.	.	.	.	✓	.	.
FMT_MTD.1/AK.eHKT_Abf	.	.	.	.	✓	.	.	.	.	.	.	.	.
FMT_MTD.1/AK.eHKT_Mod	.	.	.	.	✓	.	.	.	.	.	.	.	.
FMT_SMF.1/AK	.	.	.	.	.	.	.	.	.	.	✓	.	.
FMT_SMR.1/AK	.	.	.	.	.	.	.	.	.	.	✓	.	.
FPT_FLS.1/AK	.	.	.	.	.	.	.	.	.	.	.	✓	.
FPT_STM.1/AK	.	.	.	.	.	.	.	.	.	.	.	.	✓
FPT_TDC.1/AK	.	.	.	.	.	.	.	.	.	.	.	✓	.
FPT_TEE.1/AK	.	.	.	.	✓	✓	.	.	.	.	.	.	.
FPT_TST.1/AK.Out-Of-Band	.	.	.	.	.	.	.	.	.	.	.	✓	.
FPT_TST.1/AK.Run-time	.	.	.	.	.	.	.	.	.	.	.	✓	.
FTA_TAB.1/AK.Jobnummer	.	.	.	.	.	.	✓	.	.	.	.	.	.
FTA_TAB.1/AK.SP	.	.	.	.	.	.	✓	.	.	.	.	.	.
FTP_ITC.1/AK.CS	.	✓	.	.	.	.	.	.	.	.	.	.	.
FTP_ITC.1/AK.eHKT	.	✓	.	.	✓	.	.	.	.	.	.	.	.
FTP_ITC.1/AK.FD	.	✓	.	.	.	.	.	.	.	.	.	.	.
FTP_ITC.1/AK.KSR	.	✓	.	.	.	.	.	.	.	.	.	.	.
FTP_ITC.1/AK.TSL	.	✓	.	.	.	.	.	.	.	.	.	.	.
FTP_ITC.1/AK.QSEE	.	.	.	.	.	.	✓	.	.	.	.	.	.
FTP_ITC.1/AK.VZD	.	✓	.	.	.	.	.	.	.	.	.	.	.

Tabelle 7.3.: Abbildung der SFR des AK auf Sicherheitsfunktionalität

8. ASE_TSS: Fachmodule

Dieses Kapitel erfüllt die Anforderung des Refinements für ASE_TSS an den *Hersteller*, die in Abschnitt 6.4.5 erhoben wird.

Konnektoren dienen als Ablaufplattform für Fachmodule. Die gematik Spezifikation bezeichnet ein Fachmodul als „integrale[n] Bestandteil des Konnektors“. Daraus ergeben sich gegenseitige Anforderungen zwischen Basiskonnektor und den Fachmodulen. Dieses Kapitel geht auf die Anforderungen ein und zeigt, auf welche Weise der Basiskonnektor die Forderungen der Fachmodule umsetzt und welche Funktionen den Fachmodulen zur Verfügung gestellt werden.

Fachmodule unterliegen im Konnektor Restriktionen und Auflagen. Diese werden in der Konnektor Security Guidance beschrieben [KoCo AGD_Kon-Sec]. Die dort beschriebenen Composition Requirements müssen vom Entwickler eines Fachmoduls eingehalten werden, um die Funktionsfähigkeit des Gesamtkonnektors nicht zu gefährden. Zur besseren Lesbarkeit werden die Composition Requirements in Anhang C wiederholt.

8.1. Erklärung der Konformität zu Technischen Richtlinien

8.1.1. Fachmodule NFDM und AMTS / OPB 2.1

Die Technischen Richtlinien der Fachmodule NFDM und AMTS fordern, dass die CC-Zertifizierung des Konnektors bestimmte Eigenschaften des Konnektors umfassen muss [TR-03154; TR-03155, Abschnitt 3.3.2]. Dieses Security Target ist konform zu diesen Anforderungen, vgl. Abschnitt 2.5. Dies sind – neben den TUCs für die Fachmodule (vgl. Abschnitt 8.2) – allgemeiner formulierte Funktionalitäten. Die folgenden Unterabschnitte benennen diese Funktionalitäten und erklären, wie das Security Target die geforderten Eigenschaften sicherstellt.

Konfigurationsparameter

Der Basiskonnektor schützt die Konfigurationsparameter von Fachmodulen vor unbefugter Modifikation. Um dies sicherzustellen, setzt das Security Target folgende Maßnahme um: Die Sicherheitsfunktion SF.Administration/AK managt die Konfigurationsparameter der Fachmodule. Die Benutzung dieser Funktion wird in der Konnektor Security Guidance erklärt und dort durch Composition Requirements formalisiert [KoCo AGD_Kon-Sec].

Protokollierungsdienst

Fachmodule können den Basiskonnektor aufrufen, um Log-Nachrichten zu persistieren. Jedes Fachmodul erhält einen eigenen Namensraum, sodass die Nachrichten pro Fachmodul separiert werden. Der Konnektor speichert die Lognachrichten in derselben Datenbank wie sein eigenes Log. Benutzer der Fachmodule können über die Funktionen der Managementschnittstelle das Log auslesen. Maßnahmen des Security Targets stellen sicher, dass die Anforderungen der Fachmodule an den Konnektor umgesetzt werden:

- ST-Anwendungshinweis 53 zu FAU_STG.4/AK präzisiert die Behandlung des Parameters *FM_<fm-Name>_LOG_DAYS*, der vorgibt, wie lange die Mindestdauer für das Vorhalten von Protokolleinträgen ist [gemSpec_Kon, TAB_KON_609]. Die Konnektor Security Guidance definiert das Composition Requirement COMP-REQ-7, das beschreibt, wie der Entwickler der Fachmodule mit Konfigurationsdaten umgehen muss.
- Die Zuweisung an FAU_GEN.1.1/AK sichert zu, dass die Security-relevanten Ereignisse des Fachmoduls vom Protokollierungsdienst des Konnektors erfasst und behandelt werden.

Signaturdienst (nur für NFDM)

Fachmodule können den Signaturdienst des Basiskonnektors nutzen, um QES-Prüfungen von XML-detached Signaturen durchzuführen. Das Security Target stellt dies sicher durch die SFR in Abschnitt 6.3.3.4, insbesondere FDP_DAU.2.2/AK.QES(1), (2), (4), (5).

Gültigkeitsprüfung der eGK

Der Basiskonnektor prüft die Gültigkeit einer eGK. Dies wird erreicht durch die Erfüllung der Sicherheitsanforderung FPT_TEE.1/AK. Die Erläuterung des Sicherheitsziels O.AK.Chipkartendienst im Schutzprofil präzisiert dieses SFR [BSI-CC-PP-0098, S. 316] und macht deutlich, welche Aspekte des SFR hier einschlägig sind. Die Sicherheitsfunktionalität SF.SmartCardMgmt setzt das SFR um (vgl. Abschnitt 7.2.6).

Transportsicherung zwischen Konnektor und Clientsystem

Der Konnektor sichert die Verbindungen zu den Clientsystemen durch TLS ab[1]. Dies wird auf zwei Ebenen erreicht:

- Die Sicherheitsfunktionalität SF.CryptographicServices/NK und die damit assoziierten SFR FTP_ITC.1/NK.TLS, FPT_TDC.1/NK.TLS.Zert, 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.1/NK.Zert, FDP_ITC.2/NK.TLS und FDP_ETC.2/NK.TLS stellen die kryptographischen Eigenschaften der TLS-Verbindungen bereit.
- Die Sicherheitsfunktionalität SF.TLS managt die Verwendung der TLS-Verbindungen und reagiert auf die entsprechenden Konfigurationsparameter (vgl. Abschnitt 7.2.2). Zusätzlich trägt FMT_MOF.1/NK.TLS auch noch Anforderungen an das Management von TLS-Verbindungen bei.

Auslesbarkeit der Version des Konnektors

Die Technischen Richtlinien fordern ein „auslesbare, eindeutige Version des Konnektors sowie des Fachmoduls“. Die Auslesbarkeit ist gegeben über die Managementschnittstelle des TOE. Die Details sind dem Administratorhandbuch zu entnehmen [KoCo AGD_ADM, Abschnitte 7.4.1, 7.7.3, 7.7.4].

8.2. Umsetzung der TUCs an LS.FM im Basiskonnektor

Die Technischen Richtlinien fordern die Umsetzung von TUCs aus der Konnektor Spezifikation [gemSpec_Kon]. Tabelle 8.1 zeigt, welche SFR des Konnektors welchen TUC umsetzen und welches der Fachmodule die TUCs nutzt. Dies geschieht hier bewusst auf einer abstrakten Ebene. Tabelle 8.2 geht genauer auf die API-Funktionen ein.

[1] Die Verwendung von TLS für die Verbindung zu den Clientsystemen kann abgeschaltet werden. In diesem Fall geht die Verantwortlichkeit für die Sicherstellung der Vertraulichkeit, der Integrität und der Authentizität auf den Leistungserbringer über, vgl. [KoCo AGD_ADM, Abschnitt 7.5.1, S. 88ff].

TUC	Beschreibung	SFR	*NFDM*	*AMTS*
TUC_KON_000	Prüfe Zugriffsberechtigung	FDP_ACC.1/AK.Infomod, FDP_ACF.1/AK.Infomod	✓	✓
TUC_KON_080	Dokument validieren (wird implizit aufgerufen)	FDP_ITC.2/AK.Sig, FMT_MSA.1/AK.User	✓	.
TUC_KON_005	Card-to-Card authentisieren	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD, FIA_UAU.5/AK, FMT_MTD.1.1/AK.Zert, FMT_MTD.1/AK.Zert	✓	✓
TUC_KON_006	Datenzugriffsaudit eGK schreiben	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_012	PIN verifizieren	FDP_ACC.1/AK.PIN, FDP_ACF.1/AK.PIN	✓	✓
TUC_KON_018	eGK-Sperrung prüfen	FPT_TEE.1/AK	✓	✓
TUC_KON_022	Liefere PIN-Status	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_026	Liefere CardSession	FDP_ACC.1/AK.Infomod, FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD, FDP_ACF.1/AK.Infomod	✓	✓
TUC_KON_036	Liefere Fachliche Rolle	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_202	Lese Datei	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_203	Schreibe Datei	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_204	Lösche Datei Inhalt	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	✓
TUC_KON_051	Mit Anwender über Kartenterminal interagieren	FDP_ACC.1/AK.eHKT, FDP_ACF.1/AK.eHKT	✓	✓
TUC_KON_151	QES-Dokumentensignatur prüfen	FDP_ACC.1/AK.SigPr, FDP_ACF.1/AK.SigPr, FDP_DAU.2/AK.QES	✓	.
TUC_KON_162	Kryptographische Prüfung der XML-Dokumentensignatur	FCS_COP.1/AK.XML.SigPr	✓	.
TUC_KON_254	Liefere Ressourcendetails	FDP_ACC.1/AK.Infomod, FDP_ACF.1/AK.Infomod	✓	✓
TUC_KON_271	Schreibe Protokolleintrag	FAU_GEN.1/NK.SecLog	✓	✓
TUC_KON_351	Liefere Systemzeit	FPT_STM.1/AK, FPT_STM.1/NK	✓	✓
TUC_KON_034	Zertifikatsinformationen extrahieren	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD	✓	.

Tabelle 8.1.: Umsetzung der TUCs für Fachmodule

Die gematik Spezifikation für den Konnektor [gemSpec_Kon] regelt, welche TUCs der Basiskonnektor den Fachmodulen zur Verfügung stellen muss. Tabelle 8.2 führt diese TUCs auf und bildet sie auf die Funktionen der Schnittstelle LS.FM.RMI ab.

Anmerkungen zur Tabelle

Folgende Punkte müssen bei der Interpretation der Tabelle in Betracht gezogen werden.

- Nicht alle von der Spezifikation genannnten TUCs werden in der gegenwärtigen Version des Konnektors für die Fachmodule angeboten. TUCs, bei denen die Felder „Java-Interface“ und „Methode“ nicht befüllt sind („—“), können nicht von den Fachmodulen aufgerufen werden.
- Über die von der Spezifikation geforderten TUCs hinaus gibt es Funktionen, die Fachmodule am Basiskonnektor aufrufen können. Solche Funktionen sind in der Spalte „TUC“ mit „—“ gekennzeichnet.
- Die Interfaces liegen im Package `de.koco.konnektor.ndesign.rmi.api`.
- Die Tabelle bildet lediglich die TUCs auf Methodenaufrufe ab. Die Aufrufparameter der Java-Interfaces sind in der API dokumentiert.

Basisdienst	TUC	Name des TUC	Interface	Methode
Zugriffsberechtigungs-dienst	TUC_KON_000	Prüfe Zugriffsberechtigung	IAccessAuthorizatonServiceRemote	checkAccessAuthorization()
Dienstverzeichnis-dienst	TUC_KON_041	Einbringen der Endpunktinformationen während der Bootup-Phase	IFachmodulRegistrationRemote	registerFM()
Kartenterminaldienst	TUC_KON_051	Mit Anwender über Kartenterminal interagieren	ICardterminalInfoServiceRemote	interact()
	TUC_KON_056	Karte anfordern	CardTerminalServiceInternRemote	karteAnfordern()
	TUC_KON_057	Karte auswerfen	CardTerminalServiceInternRemote	karteAuswerfen()
Kartendienst	TUC_KON_026	Liefere CardSession	ICardServiceRemote	deliverCardSession()
	TUC_KON_012	PIN verifizieren	ICardServiceRemote	verifyPin()
	TUC_KON_019	PIN ändern	ICardServiceRemote	changePin()
	TUC_KON_021	PIN entsperren	ICardServiceRemote	unblockPin()
	TUC_KON_022	Liefere PIN-Status	ICardServiceRemote	getPinStatus()
	TUC_KON_027	PIN-Schutz ein-/ausschalten	ICardServiceRemote	toggleVerificationRequirement()
	TUC_KON_023	Karte reservieren	ICardServiceRemote	reserveCard()
	TUC_KON_005	Card-to-Card authentisieren	ICardServiceRemote	cardToCard()
	TUC_KON_202	Lese Datei	ICardServiceRemote	readFile()
	TUC_KON_203	Schreibe Datei	ICardServiceRemote	writeFile()
	TUC_KON_204	Lösche Datei Inhalt	ICardServiceRemote	deleteFileContent()
	TUC_KON_209	Lese Record	ICardServiceRemote	readRecord()
	TUC_KON_210	Schreibe Record	ICardServiceRemote	writeRecord()
	TUC_KON_211	Lösche Record Inhalt	ICardServiceRemote	eraseRecord()
	TUC_KON_214	Füge Hinzu Record	ICardServiceRemote	addRecord()
	TUC_KON_215	Suche Record	ICardServiceRemote	searchRecord()
	TUC_KON_018	eGK-Sperrung prüfen	ICardServiceRemote	checkEGKLock()
	TUC_KON_006	Datenzugriffsaudit eGK schreiben	ICardServiceRemote	writeAccessAudit()
	TUC_KON_218	Signiere	ICardServiceRemote	signPKCS1V15()
	TUC_KON_218	Signiere	ICardServiceRemote	signPSS()

Funktionen des Basiskonnektors für die Fachmodule

Basisdienst	TUC	Name des TUC	Interface	Methode
	TUC_KON_219	Entschlüssele	ICardServiceRemote	decrypt()
	TUC_KON_200	SendeAPDU	ICardServiceRemote	sendAPDU()
	TUC_KON_024	Karte zurücksetzen	ICardServiceRemote	resetCard()
	TUC_KON_216	Lese Zertifikat	ICardServiceRemote	readCertificate()
	TUC_KON_036	Liefere Fachliche Rolle	ICardServiceRemote	getProfessions()
Systeminform.-dienst	TUC_KON_256	Systemereignis absetzen	INotificationRemote	notify()
	TUC_KON_252	Liefere KT_Liste	ISystemInformationServiceRemote	getCardTerminalsFacade()
	TUC_KON_253	Liefere Karten_Liste	ISystemInformationServiceRemote	getCardsFacade()
	TUC_KON_254	Liefere Ressourcendetails	ISystemInformationServiceRemote	getResourceInformationFacade()
Verschlüsselungsdienst	TUC_KON_070	Daten hybrid verschlüsseln	IEncryptionServiceRemote	encryptDocument()
	TUC_KON_071	Daten hybrid entschlüsseln	IEncryptionServiceRemote	decryptDocument()
	TUC_KON_072	Daten symmetrisch verschlüsseln	IEncryptionServiceRemote	encryptDocument()
	TUC_KON_073	Daten symmetrisch entschlüsseln	IEncryptionServiceRemote	decryptDocument()
Signaturdienst	TUC_KON_160	Dokumente nonQES signieren	ISignserviceRemote	signNonQESDocument()
	TUC_KON_161	nonQES Dokumentsignatur prüfen	ISignserviceRemote	verifyDocument()
	TUC_KON_162	Kryptographische Prüfung der XML-Dokumentensignatur	ISignserviceRemote	verifyXMLDocumentSignature()
	TUC_KON_150	Dokument QES signieren	ISignserviceRemote	signQESDocument()
	TUC_KON_151	QES-Dokumentensignatur prüfen	ISignserviceRemote	verifyDocument()
Zertifikatsdienst	TUC_KON_037	Zertifikat prüfen	ICertificateServiceRemote	verifyCertificateX509NonQES()
	TUC_KON_037	Zertifikat prüfen	ICertificateServiceQESRemote	verifyCertificateX509QES()
	TUC_KON_042	CV-Zertifikat prüfen	ICertificateServiceRemote	verifyCertificate()
	TUC_KON_034	Zertifikatsinformationen extrahieren	ICertificateServiceRemote	extractCertificateInformation()
TLS-Dienst	TUC_KON_110	TLS-Verbindung aufbauen (kartenbas.)	—	—
	TUC_KON_111	Kartenbasierte TLS-Verbindung abbauen	—	—
LDAP-Proxy	TUC_KON_290	LDAP-Verbindung aufbauen	—	—

Funktionen des Basiskonnektors für die Fachmodule

Basisdienst	TUC	Name des TUC	Interface	Methode
	TUC_KON_291	Verzeichnis abfragen	—	—
	TUC_KON_292	LDAP-Verbindung trennen	—	—
	TUC_KON_293	Verzeichnisabfrage abbrechen	—	—
Protokollierungsdienst	TUC_KON_271	Schreibe Protokolleintrag	ILoggingServiceRemote	log()
	—	Auslesen der Log-Konfiguration	ILoggingServiceRemote	getConfiguration()
	—	Schreiben der Log-Konfiguration	ILoggingServiceRemote	setConfiguration()
Namensdienst	TUC_KON_361	DNS-Namen auflösen	IDNSServiceRemote	resolveFQDN()
	TUC_KON_362	Liste der Dienste abrufen	IDNSServiceRemote	listServiceNames()
	TUC_KON_363	Dienstdetails abrufen	IDNSServiceRemote	listServiceDetails()
Zeitdienst	TUC_KON_351	Liefere Systemzeit	INTPServiceRemote	getSystemTime()
StorageService	—	Löschen einer Datei	IStorageServiceRemote	deleteFile()
	—	Verzeichnis lesen	IStorageServiceRemote	listFiles()
	—	Datei lesen	IStorageServiceRemote	loadFile()
	—	Objekt lesen	IStorageServiceRemote	loadObject()
	—	Datei speichern	IStorageServiceRemote	storeFile()
	—	Objekt speichern	IStorageServiceRemote	storeObject()
Benachricht.-dienst	—	Versenden eines Events an den AK	IEventhandlerRemote	notify()
	—	EventHandler registrieren	IEventHandlerRegistrarRemote	registerEventHandler()
	—	EventHandler deregistrieren	IEventHandlerRegistrarRemote	unregisterEventHandler()

Tabelle 8.2.: Funktionen des Basiskonnektors für die Fachmodule

A. Erklärung der tabellarischen Darstellung

Tabelle A.1 zeigt die in den Tabellen dieses Dokuments verwendeten Symbole. Diese kommen in allen Tabellen zum Einsatz, in denen Entitäten der Common Criteria aufeinander abgebildet werden.

Symbol	Beschreibung
✓	Vom Schutzprofil vorgesehene Beziehung / vorgesehenes SFR
–	Nicht umgesetzte, vom Schutzprofil als optional vorgesehene Beziehung / vorgesehenes SFR
✓	Vom Security Target zusätzlich angenommene Beziehung / zusätzlich angenommenes SFR

Tabelle A.1.: Legende der Abbildungstabellen

B. TLS Verbindungen

Für die TLS-Verbindungen werden die im Schutzprofil und der gematik-Spezifikation [gemSpec_Krypt, Abschnitt 3.3.2] genannten Cipher Suiten verwendet. Der TOE beherrscht genau diese Cipher Suiten und keine darüber hinaus. Tabelle B.1 listet diese Cipher Suiten auf. Tabelle B.2 zeigt die elliptischen Kurven, die beim ECDHE Schlüsselaustausch zur Anwendung kommen.

Algorithmen / Cipher Suite	IANA ID	TLS 1.2 [RFC 5246]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	`0x00,0x33`	✓
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	`0x00,0x39`	✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	`0xc0,0x13`	✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	`0xc0,0x14`	✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	`0xc0,0x27`	✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	`0xc0,0x28`	✓
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	`0xc0,0x2f`	✓
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	`0xc0,0x30`	✓

Tabelle B.1.: Cipher Suites der TLS Verbindungen des Konnektors

Elliptische Kurve	IANA ID	Standard
secp256r1 (P-256)	`23`	[RFC 8422; ANSI X9.62]
secp384r1 (P-384)	`24`	[RFC 8422; ANSI X9.62]
brainpoolP256r1	`26`	[RFC 7027]
brainpoolP384r1	`27`	[RFC 7027]

Tabelle B.2.: Elliptische Kurven für die TLS Verbindungen des Konnektors

Der TOE kommuniziert mit anderen vertrauenswürdigen IT-Produkten über gesicherte Verbindungen. Die Integrität und die Vertrauenswürdigkeit der Verbindungen wird durch die Verwendung von TLS in der Version 1.2 und die in Tabelle B.1 genannten Algorithmen und Cipher Suiten sichergestellt. Tabelle B.4 listet die Verbindungen auf, die der Konnektor eingeht. Die Spalten dieser Tabelle werden in Tabelle B.3 beschrieben.

Spalte	Beschreibung
ID	Symbolischer Name der Verbindung
Schnittstelle	Logische Schnittstelle, deren Kommunikation abgesichert wird.
Rolle	Beschreibt, ob der Konnektor in dieser Verbindung Client oder Server ist.
Peer	Beschreibung des Partners in der TLS-Verbindung
Protokoll	Anwendungsprotokoll, das für die Verbindung genutzt wird.
Subsystem::Modul	Name des Subsystems und des Moduls, von dem die Verbindung ausgeht, bzw. das die Verbindung empfängt und behandelt.
Port	Port, den der TOE öffnet, um die Verbindung aufzubauen. Für Verbindungen, bei denen der Konnektor Server ist, steht hier eine Portnummer. Wenn der TOE Client ist, steht „dyn.“ für die ephemerische Portvergabe bei TCP-Verbindungen. „konfig.“ steht dafür, dass der Zielport konfigurierbar ist.
Schnittstelle	Logische Schnittstelle des TOE , über die die Verbindung läuft.
Identität des TOE	Zertifikat, mit dem sich der TOE gegenüber dem Peer authentisiert.
Identität des Peer	Zertifikat/Verfahren, mit dem sich der Peer gegenüber dem TOE authentisiert.
Authentifizierung des Peer durch	Verfahren, Datenquelle oder Subsystem/Modul, mit dem der TOE die Identität des Peers verifiziert.

Tabelle B.3.: Legende zu den TLS Verbindungen

ID	Schnittstelle (Protokoll)	Rolle	Peer	Subsystem::Modul	Port	Identität des TOE	Identität des Peer	Authentifizierung des Peer durch
TLS.1	LS.LAN.HTTP_MGMT	Server	Browser	Facade::Jetty-Configuration	9443	gSMC-K#2: EF.C.AK.AUT.R2048	Benutzername/Passwort	Benutzerverwaltung im TOE
TLS.2	LS.LAN.SOAP	Server	Clientsystem	Facade::Jetty-Configuration	443	gSMC-K#2: EF.C.AK.AUT.R2048	X.509 Zertifikate	*server_truststore.jks*
TLS.3	LS.LAN.SOAP	Server	Clientsystem	Facade::Jetty-Configuration	443	gSMC-K#2: EF.C.AK.AUT.R2048	HTTP Basic Authentication	Clientsystemverwaltung im TOE
TLS.4	LS.LAN.LDAP	Server	Clientsystem	LDAPProxy::Core	636	gSMC-K#2: EF.C.AK.AUT.R2048	X.509 Zertifikate	*server_truststore.jks*
TLS.5	LS.LAN.CETP	Client	Clientsystem	SystemInformation-Service::Core	konfig.	gSMC-K#2: EF.C.AK.AUT.R2048	X509 Zertifikate	*server_truststore.jks*
TLS.6	LS.LAN.SICCT	Client	eHealth Kartenterminal	CardService::de.ndesign.koco.ifd.sicct	4742	gSMC-K#2: EF.C.SAK.AUT.R2048	SMC-KT: ID.SMKT.AUT	CertificateService::Core
TLS.7	LS.WAN.SOAP	Client	Registrierungsdienst	AdminService::RegistrationService	8443	SMC-B: EF.C.HCI.AUT.R2048	C.ZD.TLS-S, 1.2.276.0.76.4.161	CertificateService::Core
TLS.8	LS.VPN_TI.LDAP	Client	Verzeichnisdienst	LDAPProxy::Core	Dyn.	n/a	C.ZD.TLS-S, 1.2.276.0.76.4.171	CertificateService::Core
TLS.9	LS.VPN_TI.HTTP	Client	BNetzAVL-Downloaddienst	CertificateService::-BNetzAVLService	Dyn.	n/a	C.ZD.TLS-S, 1.2.276.0.76.4.189	CertificateService::Core
TLS.10	LS.VPN_TI.SOAP	Client	Intermediär VSDM	FM_VSDM::TLS	Dyn.	SMC-B: EF.C.HCI.AUT.R2048	C.FD.TLS-S, 1.2.276.0.76.4.159	CertificateService::Core
TLS.11	LS.VPN_TI.HTTP	Client	KSR Update Server	AdminService::-KSR_CS_Core	Dyn.	n/a	C.ZD.TLS-S, 1.2.276.0.76.4.160	CertificateService::Core

Tabelle B.4.: TLS Verbindungen der KoCoBox MED+

C. Composition Requirements für Fachmodule

Fachmodule unterliegen im Konnektor Restriktionen und Auflagen. Diese werden in der Konnektor Security Guidance beschrieben [KoCo AGD_Kon-Sec]. Die dort beschriebenen Composition Requirements müssen vom Entwickler eines Fachmoduls eingehalten werden, um die Funktionsfähigkeit des Gesamtkonnektors nicht zu gefährden. Zur besseren Lesbarkeit werden die Composition Requirements hier wiederholt[1]. Einen präziseren Einblick mit mehr Erklärungen liefert die Konnektor Security Guidance.

COMP-REQ-1 Korrekte Benutzung des Konnektors

Das Fachmodul MUSS den Basiskonnektor entsprechend der vorliegenden Dokumentation und der Spezifikation der gematik benutzen. Das Fachmodul DARF NICHT die Sicherheitsfunktionen des Konnektors beeinträchtigen oder missbrauchen.

COMP-REQ-2 Auslieferungsformat

Das Fachmodul MUSS als Web-Anwendung entwickelt und als Web Application Archive ausgeliefert werden.

COMP-REQ-3 Registrierung am Basiskonnektor

Das Fachmodul MUSS sich gemäß TUC_KON_041 mit `IFachmodulRegistrationRemote.registerFM()` am Basiskonnektor registrieren.

COMP-REQ-4 Signaturrichtlinien

Das Fachmodul KANN während der Registrierung eigene Signaturrichtlinien in den Basiskonnektor einbringen. Das Fachmodul DARF NICHT andere Signaturrichtlinien verwenden.

COMP-REQ-5 Aufrufe des Basiskonnektors

Das Fachmodul KANN die in Tabelle 8.2 angegebenen Aufrufe des Basiskonnektors verwenden. Das Fachmodul MUSS die Schnittstelle LS.FM.RMI gemäß der Dokumentation der Java-API verwenden. Das Fachmodul DARF NICHT andere Funktionen des Basiskonnektors aufrufen.

COMP-REQ-6 Separation der Bibliotheken

Das Fachmodul MUSS Bibliotheken aus seinem eigenen Class-Loader verwenden. Es DARF NICHT auf die Bibliotheken und Klassen im Class-Loader anderer Fachmodule zugreifen.

COMP-REQ-7 Konfigurationsparameter für Logging

Das Fachmodul KANN während der Registrierung Konfigurationsfelder für Loggingparameter an den Basiskonnektor übergeben.

Das Fachmodul MUSS die Konfigurationsparameter mit der Funktion `ILoggingServiceRemote.setConfiguration()` des Basiskonnektors persistieren.

[1] Referenzen werden angepasst, um auf das Security Target statt auf die Konnektor Security Guidance zu verweisen.

COMP-REQ-8 Konfigurationsparameter

Das Fachmodul KANN während der Registrierung Konfigurationsfelder für Konfigurationsparameter an den Basiskonnektor übergeben.

Vom Basiskonnektor an das Fachmodul übergebene Konfigurationswerte MUSS das Fachmodul gemäß den Vorgaben der entsprechenden Spezifikation prüfen. Das Fachmodul MUSS die geprüften Konfigurationsparameter mit Funktionsaufrufen des Basiskonnektors persistieren.

COMP-REQ-9 Logging

Das Fachmodul KANN Meldungen in das Fachmodulprotokoll des Konnektors schreiben. Dafür MUSS sich das Fachmodul beim Basiskonnektor authentisieren.

COMP-REQ-10 gematik Schnittstellendefinitionen

Das Fachmodul KANN die Schnittstellendefinitionsdateien der gematik, die der Basiskonnektor bereitstellt, verwenden.

COMP-REQ-11 Keine Außenschnittstellen

Das Fachmodul DARF NICHT eigene Außenschnittstellen anbieten. Es MUSS zur Kommunktion mit den Clientsystemen SOAP-Verbindungen nutzen, die vom Proxy-Server des Basiskonnektors vermittelt werden.

COMP-REQ-12 Validierung der Eingabedaten

Das Fachmodul MUSS die vom Basiskonnektor übergebenen Eingabedaten selbst prüfen und validieren, um sich vor Angriffen von Clientsystemen zu schützen.

COMP-REQ-13 Verbindungen zu Drittsystemen

Das Fachmodul in der Ausbaustufe OPB 2.1 DARF NICHT unkontrollierte Verbindungen zu Drittsystemen aufbauen.

D. Anforderungen zur sicherheitstechnischen Eignung

in Abschnitt 3.2.1 des *Produkttypsteckbrief Konnektor* listet die gematik Anforderungen zur sicherheitstechnischen Eignung des Konnektors auf, die durch die CC-Evaluierung abgedeckt werden müssen. Im Folgenden werden die dort gelisteten Anforderungen auf die SFR des Schutzprofils abgebildet. Gegebenenfalls wird durch Erklärungen oder Refinements gezeigt, wie diese Relation interpretiert wird.

Die gematik fordert den Hersteller dazu auf, die Teile des Security Targets zu markieren, bei denen das Security Target die Anforderungen der Schutzprofile [BSI-CC-PP-0097; BSI-CC-PP-0098] erweitert. Diese Erweiterungen sind notwendig, da das Schutzprofil nicht alle Anforderungen der gematik Spezifikation abdeckt. Sie beziehen sich explizit auf die Differenz zwischen den Anforderungen aus dem Produkttypsteckbrief PTV2 [gemProdT_Kon_PTV2] und dem Produkttypsteckbrief PTV3 [gemProdT_Kon_PTV3_3.6.0-2]. Diese Differenz besteht aus 14 SFR, die – der besseren Übersichtlichkeit halber – in Tabelle D.1 aufgeführt werden, bevor in den Folgeabschnitten auf die einzelnen SFR aus PTV3 eingegangen wird.

Anforderung	SFR	Ergänzende Kommentare in
TIP1-A_4710	FAU_GEN.1/AK	ST-Anwendungshinweis 52
TIP1-A_5482	FPT_TDC.1/AK	ST-Anwendungshinweis 50
TIP1-A_5484	FDP_ACF.1/AK.SDS	ST-Anwendungshinweis 39
TIP1-A_5486	FDP_ACC.1/AK.PIN, FDP_ACF.1/AK.KD	(Umgesetzt durch PP-Anpassung)
TIP1-A_5505	FDP_DAU.2/AK.QES, FDP_DAU.2/AK.Sig	SF.SignatureService (Abschnitt 7.2.7)
TIP1-A_5538	FPT_TDC.1.2/AK, FDP_ITC.2/AK.Sig	SF.SignatureService (Abschnitt 7.2.7)
TIP1-A_6025	FDP_ACF.1/AK.Update, FPT_FLS.1/AK	ST-Anwendungshinweis 29
TIP1-A_7254	FTP_ITC.1.1/AK.FD, FTP_ITC.1.1/AK.VZD	ST-Anwendungshinweise 37, 38
TIP1-A_7255	FMT_MTD.1/AK.Admin	ST-Anwendungshinweis 48
TIP1-A_7277	—	Optionale Funktionalität entfällt.
TIP1-A_7278	—	Optionale Funktionalität entfällt.
TIP1-A_7279	—	Optionale Funktionalität entfällt.
TIP1-A_7280	—	Optionale Funktionalität entfällt.
GS-A_5484	FTP_ITC.1/AK.TSL, FPT_TDC.1/AK	(Umgesetzt durch PP-Anpassung)

Tabelle D.1.: Erweiterung des ST durch neue Anforderungen aus PTV3

TIP1-A_4710 Protokollierung personenbezogener und medizinischer Daten

Die Anforderung TIP1-A_4710 wird erfüllt durch: FAU_GEN.1/AK und die Präzisierung in Anwendungshinweis 203 des Schutzprofils.

TIP1-A_5482 TUC_KON_042 „CV-Zertifikat prüfen“

Die Anforderung TIP1-A_5482 wird erfüllt durch: FPT_TDC.1/AK

TIP1-A_5484 Persistente Speicherung von Konfigurationsdaten der Fachmodule

Die Anforderung TIP1-A_5484 wird erfüllt durch: FDP_ACF.1/AK.SDS, vgl. auch die Konnektor Security Guidance [KoCo AGD_Kon-Sec, Abschnitt 3.4].

TIP1-A_5486 TUC_KON_027 „PIN-Schutz ein-/ausschalten“

Die Anforderung TIP1-A_5486 wird erfüllt durch: FDP_ACC.1/AK.PIN, FDP_ACF.1/AK.KD

TIP1-A_5505 TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“

Die Anforderung TIP1-A_5505 wird erfüllt durch: FDP_DAU.2/AK.QES, FDP_DAU.2/AK.Sig

TIP1-A_5538 Signaturrichtlinien bei QES für XML-Dokumentenformate

Die Anforderung wird durch den neu eingefügten Unterpunkt (7) zu FDP_DAU.2/AK.QES umgesetzt.

TIP1-A_6025 Zugang zur TI sperren, wenn Deadline für kritische FW- Updates erreicht

Die Anforderung TIP1-A_6025 wird erfüllt durch: FDP_ACF.1/AK.Update, FPT_FLS.1/AK. Das Refinement in FDP_ACF.1.4/AK.Update nimmt konkreten Bezug auf die Anforderung TIP1-A_6025.

TIP1-A_7255 Anzeige von Fachmodulversionen

Die Anforderung wird durch das Refinement an FMT_MTD.1.1/AK.Admin umgesetzt. Das Refinement fordert, dass die Versionsinformation eines Fachmoduls vom Administrator einsehbar ist.

GS-A_5484 TUC_PKI_036 „BNetzA-VL-Aktualisierung“

Die Anforderung GS-A_5484 wird erfüllt durch: FTP_ITC.1/AK.TSL, FPT_TDC.1/AK

Literatur

Schutzprofile und Technische Richtlinien

[BSI-CC-PP-0082-2] Bundesamt für Sicherheit in der Informationstechnik. *Card Operating System Generation 2 (PP COS GEN2). BSI-CC-PP-0082*. Common Criteria Schutzprofil (Protection Profile). Version 1.9. Bundesamt für Sicherheit in der Informationstechnik (BSI), 18. Nov. 2014.

[BSI-CC-PP-0097] Bundesamt für Sicherheit in der Informationstechnik. *Schutzprofil 1: Anforderungen an den Netzkonnektor. BSI-CC-PP-0097*. Common Criteria Schutzprofil (Protection Profile). Version 1.6.4. Bundesamt für Sicherheit in der Informationstechnik (BSI), 17. März 2020.

[BSI-CC-PP-0098] Bundesamt für Sicherheit in der Informationstechnik. *Schutzprofil 2: Anforderungen an den Konnektor. BSI-CC-PP-0098*. Common Criteria Schutzprofil (Protection Profile). Version 1.5.4. Bundesamt für Sicherheit in der Informationstechnik (BSI), 17. März 2020.

[TR-03116-1] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 1: Telematikinfrastruktur*. Technische Richtlinie BSI TR-03116-1. Technical Guideline. Version 3.20. Bundesamt für Sicherheit in der Informationstechnik (BSI), 21. Sep. 2018. URL: `https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html`.

[TR-03154] Bundesamt für Sicherheit in der Informationstechnik. *Konnektor – Prüfspezifikation für das Fachmodul NFDM*. Technische Richtlinie BSI TR-03154. Technical Guideline. Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Apr. 2019.

[TR-03155] Bundesamt für Sicherheit in der Informationstechnik. *Konnektor – Prüfspezifikation für das Fachmodul AMTS*. Technische Richtlinie BSI TR-03155. Technical Guideline. Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Apr. 2019.

Herstellerdokumente

[KoCo AGD_ADM-Erg] KoCo Connector GmbH. *Ergänzungen zum Administratorhandbuch KoCoBox MED+ Version 2.x*. Common Criteria Komponen-

te AGD_ADM. Version 1.1.1. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

[KoCo AGD_ADM] KoCo Connector GmbH. *Administratorhandbuch KoCoBox MED+ Version 2.3*. Common Criteria Komponente AGD_ADM. Version 2.3. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 14. Juli 2020.

[KoCo AGD_JSON] KoCo Connector GmbH. *JSON-Managementschnittstelle der KoCoBox MED+. Dokumentation*. Version 2.22. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

[KoCo AGD_Kon-Sec] KoCo Connector GmbH. *KoCoBox MED+ OPB 2.1 Konnektor. Konnektor Security Guidance Fachmodule NFDM und AMTS*. Programmierrichtlinien für die Entwickler von Fachmodulen. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

[KoCo ALC_DEL] KoCo Connector GmbH. *KoCoBox MED+ OPB 2.1 Konnektor. Delivery Procedures (ALC_DEL)*. Common Criteria Komponente ALC_DEL. Version 1.1.9. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

[KoCo ASE_ST-97] KoCo Connector GmbH. *KoCoBox MED+ Netzkonnektor. Security Target*. Common Criteria Komponente ASE_ST. Vorgelegt im Verfahren BSI-DSC-CC-1067 zu BSI-CC-PP-0097. 2020.

[KoCo ASE_ST-98] KoCo Connector GmbH. *KoCoBox MED+ OPB 2.1 Konnektor. Security Target*. Common Criteria Komponente ASE_ST. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

[KoCo FM-API] KoCo Connector GmbH. *KoCoBox MED+ OPB 2.1 Konnektor. Konnektor API für Fachmodule Javadoc*. Common Criteria Komponente AGD. Vorgelegt im Verfahren BSI-DSC-CC-1068 zu BSI-CC-PP-0098. 2020.

Spezifikationen

[CAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). CAdES Baseline Profile*. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103173v020101p.pdf.

[CAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). CMS Advanced Electronic Signatures (CAdES)*. ETSI Technical Specification. Version 2.2.1. ETSI, Apr. 2013. URL: http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf.

[PAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). PAdES Baseline Profile*. ETSI Technical Specification. Version 2.2.2. ETSI, Apr. 2013. URL: http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

[PAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). PDF Advanced Electronic Signature Profiles*. Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles. ETSI Technical Specification. Version 1.2.1. ETSI, Juli 2010. URL: http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf.

[TIFF] Adobe Developers Association, Hrsg. *TIFF. Revision 6.0*. Version 6.0. 3. Juni 1992. URL: https://www.adobe.io/open/standards/TIFF.html.

[XAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). XAdES Baseline Profile*. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012. URL: http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.

[XAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). XML Advanced Electronic Signatures (XAdES)*. ETSI Technical Specification. Version 1.4.2. ETSI, Dez. 2010. URL: http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf.

[XML] Tim Bray u. a. *Extensible Markup Language (XML)*. W3C Recommendation. http://www.w3.org/TR/xml. W3C, Nov. 2008.

[XMLEnc] Frederick Hirsch u. a. *XML Encryption Syntax and Processing Version 1.1*. W3C Recommendation. http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/. W3C, Apr. 2013.

[XSLT] Michael Kay. *XSL Transformations (XSLT)*. W3C Recommendation. Version 2.0. http://www.w3.org/TR/2007/REC-xslt20-20070123/. W3C, Jan. 2007.

gematik Spezifikationen

[gemErrata_1_Kon_PTV3] gematik GmbH. *Errata 1 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.1., 6. Feb. 2019.

[gemErrata_2_Kon_PTV3] gematik GmbH. *Errata 2 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.0., 6. Juni 2019.

[gemErrata_3_Kon_PTV3] gematik GmbH. *Errata 3 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.0., 2. Okt. 2019.

[gemErrata_4_Kon_PTV3] gematik GmbH. *Errata 4 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.1., 27. Nov. 2019.

[gemErrata_5_Kon_PTV3] gematik GmbH. *Errata 5 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.0., 4. Feb. 2020.

[gemErrata_6_Kon_PTV3] gematik GmbH. *Errata 6 zum Konnektor PTV 3 (eMP/AMTS, NFDM)*. Version 1.0.0., 4. März 2020.

[gemILF_PS] gematik GmbH. *Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI)*. einschließlich VSDM, QES, KOM-LE. Version 2.3.0. Revision 55792., 26. Okt. 2018.

[gemKPT_Arch] gematik GmbH. *Konzept. Architektur der TI-Plattform*. Version 2.5.0. Revision 58160., 26. Okt. 2018.

[gemProdT_Kon_PTV2] gematik GmbH. *Produkttypsteckbrief Konnektor*. Prüfvorschrift. Produkttyp Version PTV2 2.12.0-0. Version 1.0.0., 14. Mai 2018.

[gemProdT_Kon_PTV3_3.6.0-2] gematik GmbH. *Produkttypsteckbrief Konnektor*. Prüfvorschrift. Produkttyp Version PTV3 3.6.0-2. Version 1.0.0. Revision 61976., 4. März 2020.

[gemRL_QES_NFDM] gematik GmbH. *Signaturrichtlinie QES. Notfalldaten-Management (NFDM)*. Version 1.4.0. Revision 17752., 28. Juni 2019.

[gemSpec_COS] gematik GmbH. *Spezifikation des Card Operating System (COS)*. Version 3.11.0., 14. Mai 2018.

[gemSpec_FM_AMTS] gematik GmbH. *Spezifikation Fachmodul AMTS*. Version 1.3.0. Revision 57164., 26. Okt. 2018.

[gemSpec_FM_NFDM] gematik GmbH. *Spezifikation Fachmodul NFDM*. Version 1.4.0. Revision 57194., 26. Okt. 2018.

[gemSpec_HBA_ObjSys] gematik GmbH. *Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem*. Version 3.11.0. Revision 19010., 14. Mai 2018.

[gemSpec_Kon_TBAuth] gematik GmbH. *Spezifikation Konnektor. Basisdienst Tokenbasierte Authentisierung*. Version 1.2.0. Revision 19021., 14. Mai 2018.

[gemSpec_Kon] gematik GmbH. *Spezifikation Konnektor*. Version 5.4.0., 26. Okt. 2018.

[gemSpec_Krypt] gematik GmbH. *Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur*. Version 2.11.0. Revision 58823., 29. Okt. 2018.

[gemSpec_Net] gematik GmbH. *Übergreifende Spezifikation Netzwerk*. Version 1.14.0. Revision 58088., 26. Okt. 2018.

[gemSpec_PKI] gematik GmbH. *Übergreifende Spezifikation PKI*. Version 2.3.0. Revision 58259., 26. Okt. 2018.

[gemSpec_SMC-B_ObjSys] gematik GmbH. *Spezifikation der Security Module Card SMC-B Objektsystem*. Version 3.11.0. Revision 19706., 26. Okt. 2018.

[gemWSDL] gematik GmbH. *Schnittstellendefinitionen im XSD- und WSDL-Format*. Gültig ab 01.01.2019. 2019. URL: https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Produktivbetrieb/Schemata_WDSL/OPB3.1_Schemadateien_R3.1.2_Kon_PTV3_20191002.zip.

Standards

[ANSI X9.62] Accredited Standards Committee X9. *ANSI X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Standard. ANSI, 16. Nov. 2005.

[CC Part 2] The Common Criteria Recognition Agreement Members. *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components*. Common Criteria. Version 3.1R5. Common Criteria Portal, Apr. 2017. URL: http://www.commoncriteriaportal.org/thecc.html.

[CC Part 3] The Common Criteria Recognition Agreement Members. *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components*. Common Criteria. Version 3.1R5. Common Criteria Portal, Apr. 2017. URL: http://www.commoncriteriaportal.org/thecc.html.

[FIPS PUB 180-4] National Institute of Standards und Technology. *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Aug. 2015. URL: http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[FIPS PUB 186-2] National Institute of Standards und Technology. *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Juli 2013. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[FIPS PUB 197] National Institute of Standards und Technology. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Nov. 2001. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[ISO 19005-1] ISO. *Document management – Electronic document file format for long-term preservation. Part 1: Use of PDF 1.4 (PDF/A-1)*. International Standard. International Organization for Standardization, 28. Sep. 2005.

[ISO 19005] ISO. *Document management – Electronic document file format for long-term preservation*. International Standard. International Organization for Standardization, 2005.

[ISO 8859-15] ISO. *Information technology – 8-bit single-byte coded graphic character sets. Part 15: Latin alphabet No. 9*. International Standard. International Organization for Standardization, 12. Feb. 2004.

[NIST SP 800-133] Elaine Barker und Allen Roginsky. *Recommendation for Cryptographic Key Generation*. NIST Special Publication 800-133. National Institute of Standards und Technology, Dez. 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf.

[NIST SP 800-38A] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. Methods and Techniques*. NIST Special Publication 800-38A. National Institute of Standards und Technology, Dez. 2001. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf.

[NIST SP 800-38D] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800-38D. National Institute of Standards und Technology, Nov. 2007. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

[NIST SP 800-90A] Elaine Barker und John Kelsey. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators. National Industrial Security Program Operating Manual*. NIST Special Publication. Version Revision 1. National Institute of Standards und Technology, Juni 2015. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.

[Unicode] The Unicode Consortium. *The Unicode Standard. Core Specification*. Version 6.2. Hrsg. von Julie D. Allen u. a. Mountain View, CA, 2012. ISBN: 978-1-936213-07-8. URL: http://www.unicode.org/versions/Unicode6.2.0.

RFC

[RFC 2131] R. Droms. *Dynamic Host Configuration Protocol*. RFC 2131 (Draft Standard). RFC. Updated by RFCs 3396, 4361, 5494, 6842. Fremont, CA, USA: RFC Editor, März 1997. DOI: 10.17487/RFC2131. URL: https://www.rfc-editor.org/rfc/rfc2131.txt.

[RFC 2132] S. Alexander und R. Droms. *DHCP Options and BOOTP Vendor Extensions*. RFC 2132 (Draft Standard). RFC. Updated by RFCs 3442, 3942, 4361, 4833, 5494. Fremont, CA, USA: RFC Editor, März 1997. DOI: 10.17487/RFC2132. URL: https://www.rfc-editor.org/rfc/rfc2132.txt.

[RFC 2404] C. Madson und R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Nov. 1998. DOI: 10.17487/RFC2404. URL: https://www.rfc-editor.org/rfc/rfc2404.txt.

[RFC 3526] T. Kivinen und M. Kojo. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. RFC 3526 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Mai 2003. DOI: 10.17487/RFC3526. URL: https://www.rfc-editor.org/rfc/rfc3526.txt.

[RFC 4035] R. Arends u. a. *Protocol Modifications for the DNS Security Extensions*. RFC 4035 (Proposed Standard). RFC. Updated by RFCs 4470, 6014, 6840. Fremont, CA, USA: RFC Editor, März 2005. DOI: 10.17487/RFC4035. URL: https://www.rfc-editor.org/rfc/rfc4035.txt.

[RFC 4055] J. Schaad, B. Kaliski und 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*. RFC 4055 (Proposed Standard). RFC. Updated by RFC 5756. Fremont, CA, USA: RFC Editor, Juni 2005. DOI: 10.17487/RFC4055. URL: https://www.rfc-editor.org/rfc/rfc4055.txt.

[RFC 4868] S. Kelly und S. Frankel. *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*. RFC 4868 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Mai 2007. DOI: 10.17487/RFC4868. URL: https://www.rfc-editor.org/rfc/rfc4868.txt.

[RFC 5246] T. Dierks und E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246 (Proposed Standard). RFC. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905, 7919. Fremont, CA, USA: RFC Editor, Aug. 2008. DOI: 10.17487/RFC5246. URL: https://www.rfc-editor.org/rfc/rfc5246.txt.

[RFC 5280] D. Cooper u. a. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 (Proposed Standard). RFC. Updated by RFC 6818. Fremont, CA, USA: RFC Editor, Mai 2008. DOI: 10.17487/RFC5280. URL: https://www.rfc-editor.org/rfc/rfc5280.txt.

[RFC 5639] M. Lochter und J. Merkle. *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. RFC 5639 (Informational). RFC. Fremont, CA, USA: RFC Editor, März 2010. DOI: 10.17487/RFC5639. URL: https://www.rfc-editor.org/rfc/rfc5639.txt.

[RFC 5652] R. Housley. *Cryptographic Message Syntax (CMS)*. RFC 5652 (Internet Standard). RFC. Fremont, CA, USA: RFC Editor, Sep. 2009. DOI: 10.17487/RFC5652. URL: https://www.rfc-editor.org/rfc/rfc5652.txt.

[RFC 5746] E. Rescorla u. a. *Transport Layer Security (TLS) Renegotiation Indication Extension*. RFC 5746 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Feb. 2010. DOI: 10.17487/RFC5746. URL: https://www.rfc-editor.org/rfc/rfc5746.txt.

[RFC 5751] B. Ramsdell und S. Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*. RFC 5751 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Jan. 2010. DOI: 10.17487/RFC5751. URL: https://www.rfc-editor.org/rfc/rfc5751.txt.

[RFC 5905] D. Mills u. a. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. RFC 5905 (Proposed Standard). RFC. Updated by RFC 7822. Fremont, CA, USA: RFC Editor, Juni 2010. DOI: 10.17487/RFC5905. URL: https://www.rfc-editor.org/rfc/rfc5905.txt.

[RFC 7027] J. Merkle und M. Lochter. *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)*. RFC 7027 (Informational). RFC. Fremont, CA, USA: RFC Editor, Okt. 2013. DOI: 10.17487/RFC7027. URL: https://www.rfc-editor.org/rfc/rfc7027.txt.

[RFC 7292] K. Moriarty u. a. *PKCS #12: Personal Information Exchange Syntax v1.1*. RFC 7292 (Informational). RFC. Fremont, CA, USA: RFC Editor, Juli 2014. DOI: 10.17487/RFC7292. URL: https://www.rfc-editor.org/rfc/rfc7292.txt.

[RFC 7296] C. Kaufman u. a. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 7296 (Internet Standard). RFC. Updated by RFCs 7427, 7670. Fremont, CA, USA: RFC Editor, Okt. 2014. DOI: 10.17487/RFC7296. URL: https://www.rfc-editor.org/rfc/rfc7296.txt.

[RFC 8017] K. Moriarty (Ed.) u. a. *PKCS #1: RSA Cryptography Specifications Version 2.2*. RFC 8017 (Informational). RFC. Fremont, CA, USA: RFC Editor, Nov. 2016. DOI: 10.17487/RFC8017. URL: https://www.rfc-editor.org/rfc/rfc8017.txt.

[RFC 8422] Y. Nir, S. Josefsson und M. Pegourie-Gonnard. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. RFC 8422 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2018. DOI: 10.17487/RFC8422. URL: https://www.rfc-editor.org/rfc/rfc8422.txt.

Andere

[BÄK-DV] Bundesärztekammer. „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“. In: *Deutsches Ärzteblatt* 111.21 (23. Mai 2014). URL: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/Schweigepflicht_2014.pdf (besucht am 04. 07. 2017).

[BSI-GS] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz-Kataloge*. 2017. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

[ESSIV] Clemens Fruwirth. *New Methods in Hard Disk Encryption*. 18. Juli 2005. URL: http://clemens.endorphin.org/nmihde/nmihde-A4-os.pdf.

[RUB-XML] Meiko Jensen u. a. „On the Effectiveness of XML Schema Validationfor Countering XML Signature Wrapping Attacks“. In: *XML Schema Validation* 7.1 (1. Jan. 2013). URL: https://www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2013/03/25/paper.pdf (besucht am 18. 12. 2019).

Verzeichnis der ST-Anwendungshinweise

Index der SFR