Common Criteria Certification
BSI-DSZ-CC-1067-V5 BSI-CC-PP-0097

Security Target

Netzkonnektor

KoCoBox MED+ Netzkonnektor
Version 5.5.12

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

Dokumentversion 4.10
02.09.2024

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 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 [ASE_ST-98] enthält auch den gesamten Inhalt des Security Targets für den Netzkonnektor [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 [ASE_ST-97] beschrieben sind, ebenfalls auf beide Schutzprofile.*

Ziel dieser Maßnahme ist, dass ein Evaluator lediglich die Dokumente für den Gesamtkonnektor [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 Spezifikationslage

Die KoCoBox MED+ wurde nach der Spezifikation der gematik entwickelt. Dabei gelten die Spezifikationsdokumente, die für den Konnektor im „Produkttypsteckbrief Konnektor“ Produkttyp Version PTV5Plus 5.54.1-0 1.0.0 genannt werden [gemProdT_Kon_PTV5P].

Die Laufzeitverlängerung ist gemäß der separaten Spezifikation „Feature Laufzeitverlängerung gSMC-K“ in Version 1.2.0 umgesetzt [gemF_LZV_gSMC-K].

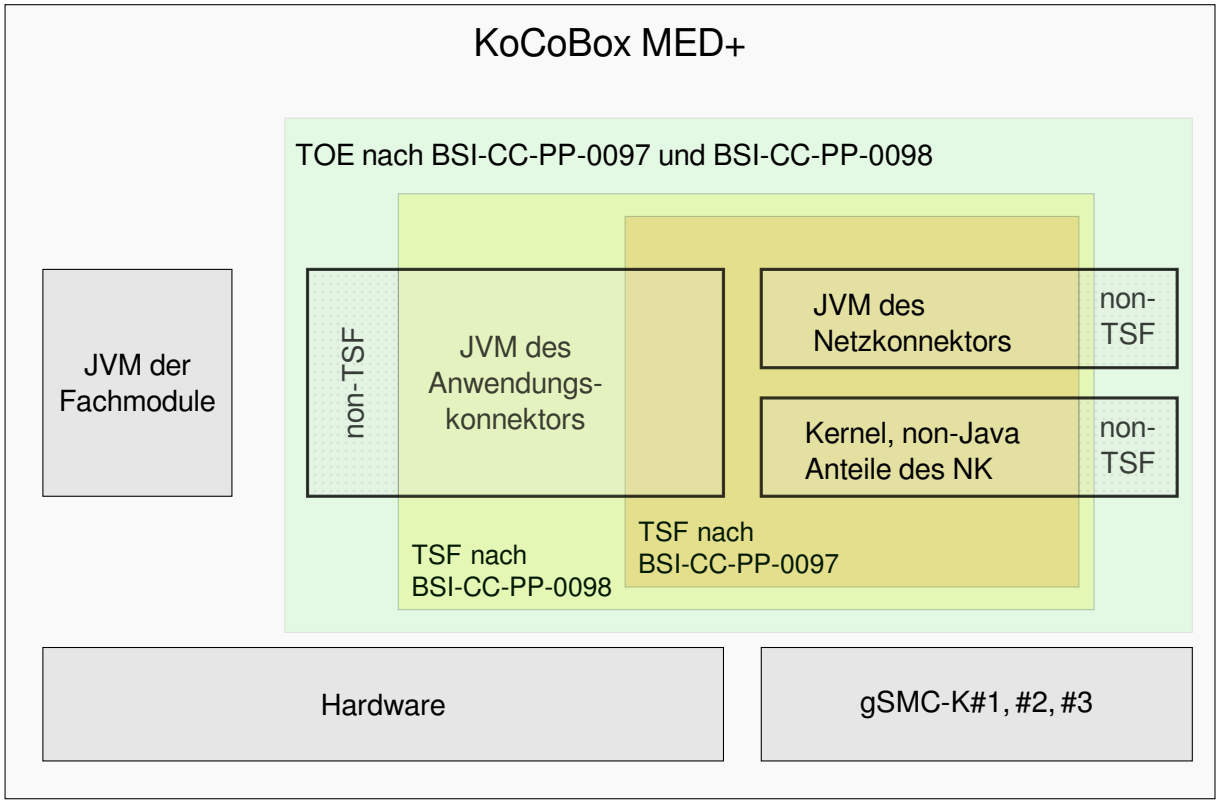


Abbildung 1.: Abgrenzung der Verfahren zu BSI-CC-PP-0097 und BSI-CC-PP-0098

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einführung in das Security Target

Der TOE, der in diesem Dokument beschrieben wird, ist der *KoCoBox MED+ Netzkonnektor*. Der TOE ist eine sichere Komponente, die im Kontext der Telematikinfrastruktur als Netzkonnektor 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 1: Anforderungen an den Netzkonnektor* [BSI-CC-PP-0097]

Darüber hinaus gibt es – wie im Vorwort beschrieben – eine enge Verwandtschaft zum Dokument *Schutzprofil 2: Anforderungen an den Konnektor* [BSI-CC-PP-0098].

1.1. ST Referenz

Titel des Dokuments	Security Target / Netzkonnektor
Version des Dokuments	4.10
Datum des Dokuments	02.09.2024
Autor	KoCo Connector GmbH
Editor	CGM Köln, os-cillation

1.2. TOE Referenz

Evaluierungsgegenstand	KoCoBox MED+ Netzkonnektor
Version des EVG	5.5.12
Hersteller	KoCo Connector GmbH
Vertrauenswürdigkeitsstufe	EAL3 erweitert um AVA_VAN.5, 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 in der Produkttypversion PTV 5+. Der TOE umfasst folgende Komponenten:

- den Netzkonnektor

Der Lieferumfang des TOE umfasst ebenfalls die Betriebsdokumentation für den Netzkonnektor. Somit entspricht der TOE dem im Schutzprofil [BSI-CC-PP-0097] genannten Umfang und Aufbau.

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 (vgl. Literaturverzeichnis, besonders aber [gemSpec_Krypt]). Die Sicherheitsanforderungen spezifiziert das Schutzprofil [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.[1] 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 Hardware liegt in zwei Gerätegenerationen vor: Generation 3 (G3) und Generation 4 (G4).

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 dabei logisch an den Konnektor gekoppelt. Sie sind nicht durch neue oder andere Karten gleichen Typs austauschbar.[2] Weder Endbenutzer noch geschultes Service-Personal können die gSMC-K ersetzen. Die Manipulation oder das Entfernen der Smart Cards führt zur Außerbetriebsetzung des Geräts. Die Smart Cards sind nicht 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] Im folgenden wird der Einfachheit halber angenommen, dass die Einsatzumgebung eine Arztpraxis ist.

[2] Es werden keine Maßnahmen umgesetzt, die das Entfernen der gSMC-K verhindern, vgl. die Definition der Annahme A.NK.phys_Schutz im Schutzprofil [BSI-CC-PP-0097].

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 *das erste dieser 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 Signaturanwendungskomponente 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.

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

[3] oder eine andere Zugangstechnologie

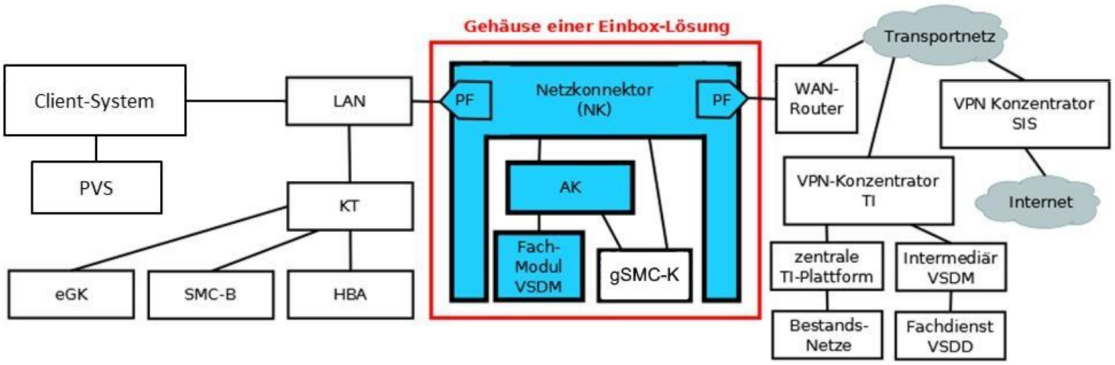


Abbildung 1.1.: Einsatzumgebung der KoCoBox MED+

ein Gerät, bei dem alle relevanten Komponenten in einem einzigen Gehäuse untergebracht sind. Das Gehäuse enthält sowohl den Netz-, als auch den Anwendungskonnektor.

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 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 1.1 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]

Im LAN des Leistungserbringers geht der TOE Verbindungen zu anderen IT-Produkten ein: Den Clientsystemen und den eHealth-Kartenterminals. Die Verbindung zwischen dem Konnektor und den kontrollierten eHealth Kartenterminals ist durch gegenseitige Authentisierung abgesichert. Die Verbindung zu den Clientsystemen ist standardmäßig durch TLS und Clientauthentisierung abgesichert.

[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.

Der Administrator kann für die Verbindung zu den Clientsystemen auf Authentisierung und auch auf Verschlüsselung verzichten. Im letzteren Fall geht die Verantwortung für den sicheren Betrieb auf den Leistungserbringer über. Weiterhin ist die Benutzung des Merkmals Komfortsignatur nur möglich, wenn Verschlüsselung und Clientauthentisierung aktiviert sind.

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. Die Hardware liegt in zwei Gerätegenerationen vor: Generation 3 (G3) und Generation 4 (G4). Auf die Hardware wird weiter unter unten genauer eingegangen.

3 × Smart Card gSMC-K Vertrauenswürdige Smart Cards vom Typ gSMC-K. Der Konnektor unterstützt drei Karten dieser Art, um die Performance bei kryptographischen Operationen zu steigern. Es kommen unterschiedliche SmartCards zum Einsatz. In der G3-Hardware werden ausschließlich Karten vom Typ STARCOS 3.6 verwendet. Die G4-Hardware hingegen wird mit Karten der Typen STARCOS 3.7 oder TCOS FlexCert 2.0 bestückt, wobei innerhalb eines Konnektors immer Karten desselben Typs verwendet werden.

Gen.	Hersteller	COS	Zertifikat	Security Target
G3[†]	G+D	STARCOS 3.6 COS C1	BSI-DSZ-CC-0916-2015	[STARCOS-ST_36]
G4	G+D	STARCOS 3.7 COS HBA-SMC	BSI-DSZ-CC-0976-V4-2021	[STARCOS-ST_37]
	T-Systems	TCOS FlexCert 2.0 Release 2	BSI-DSZ-CC-0904-V2-2021	[TCOS-ST]

[†] Während Karten für die Hardwaregeneration 4 immer dual-personalisiert sind, d. h. sowohl RSA- als auch ECC-Zertifikate und -Schlüsselmaterial enthalten, ist dies bei in G3-Konnektoren verbauten Karten unterschiedlich. Welche Schlüsseltypen auf den Karten eines Konnektors vorhanden sind, lässt sich indirekt über die verfügbaren Zertifikate (einsehbar über die Managementoberfläche) ermitteln. Die Smart Cards sind anhand ihrer Seriennummer unterscheidbar. Bis zur Nummer 80276003640000095102 enthalten diese ausschließlich RSA-Material. Karten mit höheren Seriennummern verfügen über RSA- und ECC-Material.

Telematikinfrastruktur Die TI wird von der gematik bereitgestellt. Die TI wird über die Spezifikationen der gematik definiert.

SIS Der sichere Internet-Service ist ein dedizierter VPN-Konzentrator, der über das WAN Interface des Konnektors erreichbar ist. Der SIS wird über die Spezifikation der gematik 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-TI]. 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+

Der TOE kann nur auf den definierten Hardware-Plattformen des Herstellers betrieben werden. Es gibt zwei Generationen dieser Hardware: die Generation 3 (G3) und die Generation 4 (G4). Beide Plattformen sind architekturell ähnlich, sodass der Großteil der Beschreibungen für beide Generationen anwendbar ist. Die spezifischen Eigenschaften der jeweiligen Generation werden weiter unten in eigenen Abschnitten beschrieben.

Beide Generationen bestehen aus einem System-on-a-chip (SoC) und zusätzlichen Komponenten für Ein- und Ausgabe. Alle Teile des TOE werden durch die CPU des System-on-a-chip ausgeführt. Insbesondere die Schnittstellen des TOE sind aus Sicht der Sicherheitsleistungen identisch aufgebaut.

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.

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 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 werden. 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 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 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

Abbildung 1.2.: Gehäuse der Generation 3 (G3)

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.

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.

1.4.4.1. Hardware der Generation 3 (G3)

Abbildung 1.2 zeigt das Gehäuse der der Generation 3 der KoCoBox MED+. Abbildung 1.3 auf Seite 15 bildet die Hardware-Komponenten ab, aus denen sich die Laufzeitumgebung des TOE zusammensetzt.

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.

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

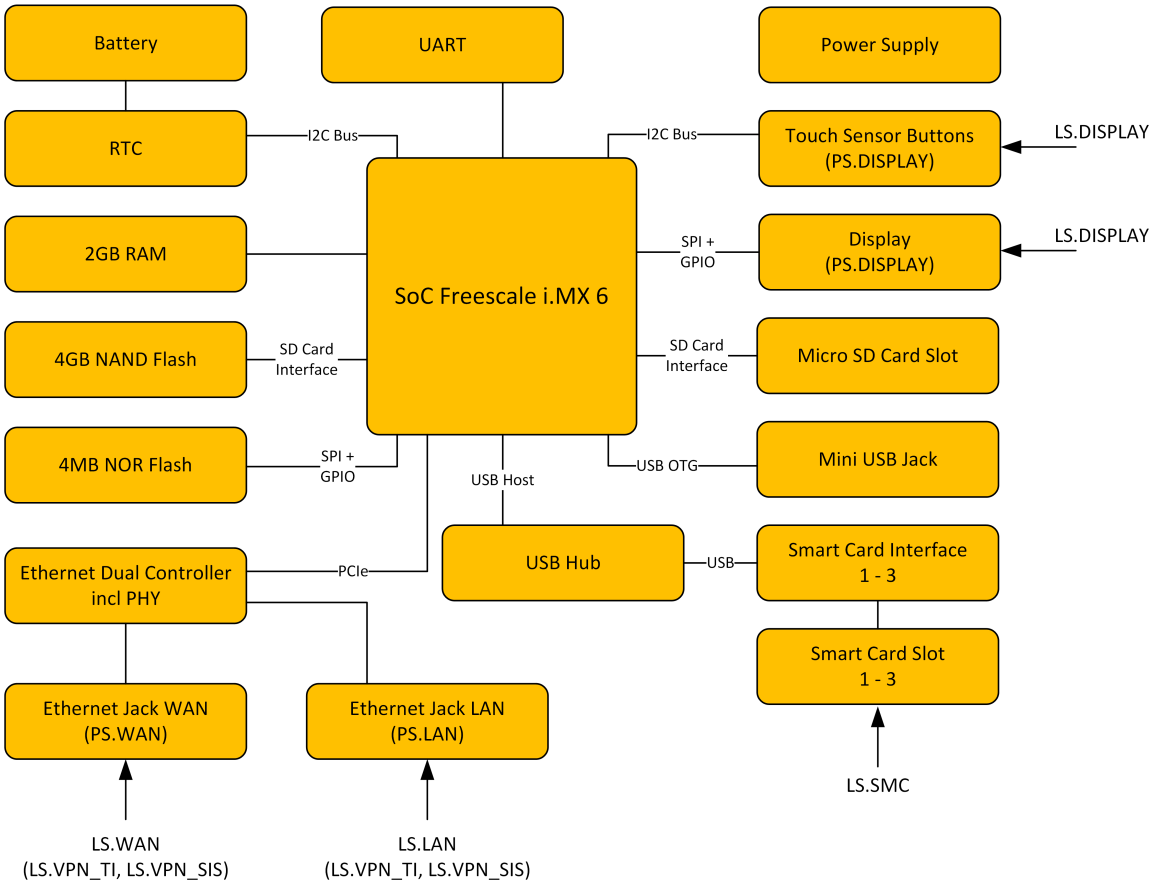


Abbildung 1.3.: Hardware-Komponenten der Generation 3 (G3). Die logischen Schnittstellen des TOE sind in dem Diagramm als von außen an die Systemkomponenten heranreichende Pfeile repräsentiert. Die entsprechenden physischen Schnittstellen sind in den äußeren Komponenten eingetragen.

und das Initramfs und dann im Initramfs alle anderen Firmwareanteile auf ihre Integrität geprüft.

Abbildung 1.4.: Gehäuse der KoCoBox MED+ (G4)

1.4.4.2. Hardware der Generation 4 (G4)

Abbildung 1.4 zeigt das Gehäuse der der Generation 4 der KoCoBox MED+. Abbildung 1.5 auf Seite 18 bildet die Hardware-Komponenten ab, aus denen sich die Laufzeitumgebung des TOE zusammensetzt.

Die 8 GB RAM bilden den flüchtigen Arbeitsspeicher. Der persistente NAND-Flash Speicher befindet sich auf einer Speicherkarte (embedded Multimedia Card eMMC). Dieser Speicher ist 32 GB groß. Er wird im pSLC Modus betrieben, wodurch nur 16 GB verwendet werden können.

Das EEPROM wird zur Ablage von Gerätespezifischen Daten wie MAC-Adressen und Seriennummern verwendet.

Als zusätzliche Schutzmaßnahme prüft der SoC vor dem Start die Signatur des Bootloader (Advanced High Assurance Boot, AHAB). Danach werden durch weitere Verifizierungen von Signaturen zuerst der Kernel und das Initramfs und dann im Initramfs alle anderen Firmwareanteile auf ihre Integrität geprüft.

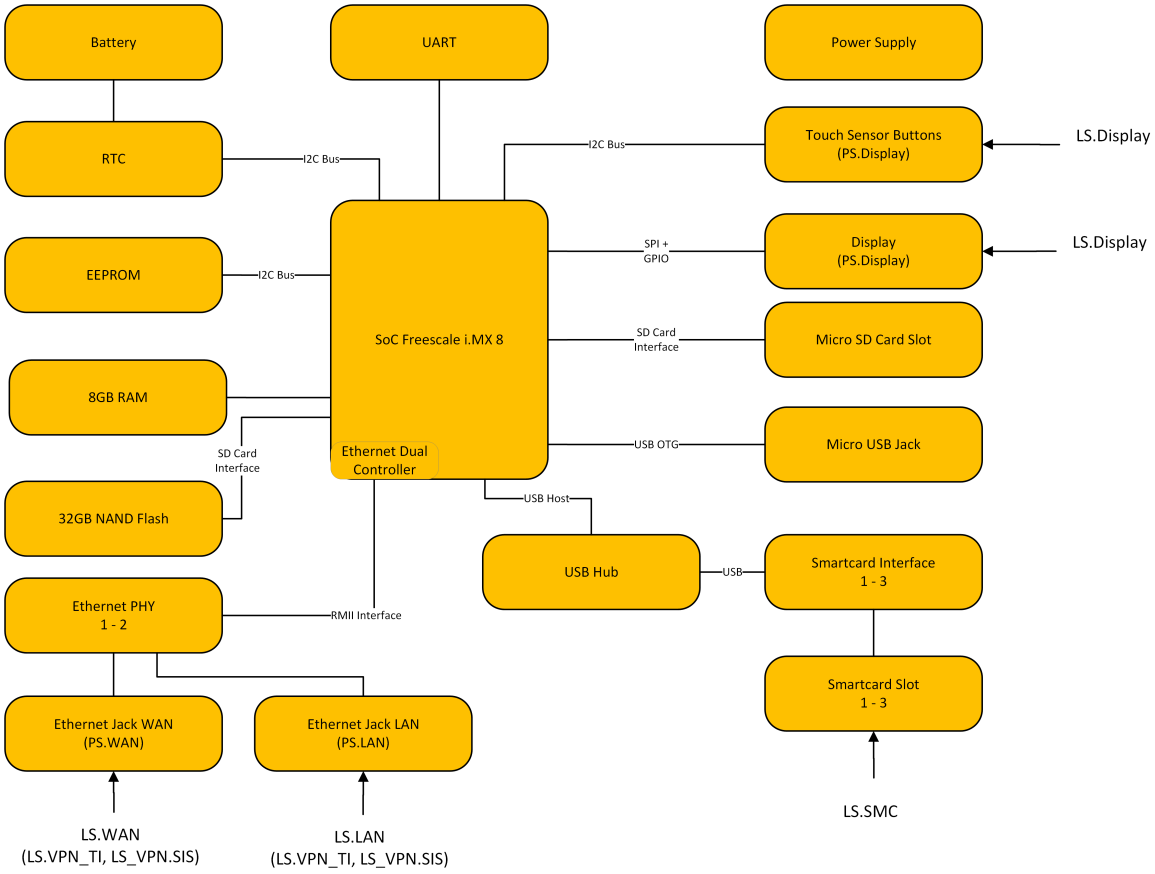


Abbildung 1.5.: Hardware-Komponenten der Generation 4 (G4). Die logischen Schnittstellen des TOE sind in dem Diagramm als von außen an die Systemkomponenten heranreichende Pfeile repräsentiert. Die entsprechenden physischen Schnittstellen sind in den äußeren Komponenten eingetragen.

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 (G3) und Abbildung 1.5 (G4) aufgeführt, die außen sichtbaren Schnittstellen sind auf dem Foto des TOE in Abbildung 1.2 (G3) und Abbildung 1.4 (G4) 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 Unterabschnitt 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 1.2 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 1.3 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 1.4 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 1.5 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 1.6 listet diese Logischen Schnittstellen.

[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.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.AuthSignatureService	Server	Zugriff auf den Authentisierungsdienst
LS.LAN.CardService	Server	Zugriff auf den Kartendienst
LS.LAN.CertificateService	Server	Zugriff auf den Zertifikatsdienst
LS.LAN.CTService	Server	Zugriff auf den Kartenterminaldienst
LS.LAN.EncryptionService	Server	Zugriff auf den Verschlüsselungsdienst
LS.LAN.SignatureService	Server	Zugriff auf den Signaturdienst
LS.LAN.SysInfService	Server	Zugriff auf den Systeminformationsdienst
LS.LAN.VSDM	Server	Zugriff auf das Versichertenstammdatenmanagement
LS.LAN.FM	Server	Zugriff auf die Fachmodule NFDM und AMTS des Konnektors
LS.LAN.ePAv1	Server	Zugriff auf das Fachmodul ePA v1.3 des Konnektors
LS.LAN.ePAv2	Server	Zugriff auf das Fachmodul ePA v2.0 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 1.2.: 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	—	Protokoll auf Anwendungsschicht
LS.WAN.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 1.3.: 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.OCSP	Client	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.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
LS.VPN_TI.VAU	Client	Kommunikation mit dem VAU-Server-Endpunkt
LS.VPN_TI.DokVerw	Client	Kommunikation mit der ePA-Dokumentenverwaltung
LS.VPN_TI.SGD	Client	Kommunikation mit dem ePA-Schlüsselgenerierungsdienst
LS.VPN_TI.Authn	Client	Kommunikation mit dem ePA-Authentisierungsdienst
LS.VPN_TI.Authz	Client	Kommunikation mit dem ePA-Autorisierungsdienst

Tabelle 1.4.: 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 1.5.: 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 1.6.: Logische Schnittstellen an LS.FM

1.4.6. Aufbau und physische Abgrenzung des Konnektors PTV 5+

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

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.

Application 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.

Fachmodule Dieses Subsystem stellt die Funktionen für das Versichertenstammdatenmanagment 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 Krypto-Framework BouncyCastle, der WebServer Jetty und der Algorithmenvalidierungsdienst.

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

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.

1.4.8. Physischer Umfang des TOE

Der physische Umfang des TOE umfasst die in Tabelle 1.7 aufgelisteten Komponenten. Der Kunde erhält die Firmware vorinstalliert auf der Hardware der KoCoBox MED+. Updates und neue Produkttypversionen werden gemäß den Vorgaben der gematik vom KSR-Server geladen. Darüber hin aus gibt es auf der Website des Herstellers einen passwortgeschützten Bereich, in dem die Firmware ebenfalls heruntergeladen werden kann. Die so erhaltenen Dateien kann der Administrator über die Managementschnittstelle einspielen und aktivieren.

Komponente/Ausprägung	Beschreibung	Version
Firmware Image (G3/G4) Typ: Binärdaten*	Die Firmware und der Boot Loader des TOE. Die Firmware umfasst den Netzkonnektor (Version 5.5.12), den Anwendungskonnektor (Version 7.15.1), die Fachmodule NFDM, AMTS und ePA (in Version 7.15.1). Für die Hardwareplattformen G3 und G4 werden unterschiedliche Images ausgeliefert.	5.5.12
Guidance Documentation („Administratorhandbuch KoCoBox MED+ Version 5“) Typ: PDF-Dokument†	Die Guidance Documentation beschreibt die sichere Verwendung des TOE [AGD_ADM].	5 (17.7.2024)
Guidance Documentation („Ergänzungen zum Administratorhandbuch KoCoBox MED+ Version 5“) Typ: PDF-Dokument†	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 [AGD_ADM-Erg].	1.3.4
Benutzerhandbuch („Allgemeine Gebrauchsanleitung KoCoBox MED+“) Typ: Booklet‡	Das Benutzerhandbuch beschreibt die allgemeine Verwendung des Konnektors, sowohl dessen TOE Anteile als auch die nicht-TOE Anteile.	1.3.8 (G3) 2.1 (G4)
Entwicklerhandbuch („JSON-Managementschnittstelle der KoCoBox MED+“) Typ: PDF-Dokument×	Anleitung für die Benutzung der API von `LS.LAN.HTTP_MGMT`. Zur internen Verwendung, wird nicht an Endkunden ausgeliefert.	3.22
Konnektor Security Guidance Fachmodule NFDM, AMTS und ePA Typ: PDF-Dokument×	Anleitung zur Verwendung des Konnektors für die Autoren der Fachmodule AMTS, NFDM und ePA [AGD_Kon-Sec]. Zur internen Verwendung, wird nicht an Endkunden ausgeliefert.	4.3
Konnektor API für Fachmodule Javadoc Typ: HTML-Seiten×	API-Beschreibung der Funktionen des Basiskonnektors für Fachmodule. Zur internen Verwendung, wird nicht an Endkunden ausgeliefert.	7.15.1

* Die initiale Auslieferung erfolgt über die Hardware der KoCoBox MED+. Neue Versionen werden in der Regel über den KSR-Server der TI ausgeliefert. Die Firmware wird auch über die Website des Herstellers verteilt.

† Wird über die Website des Herstellers verteilt.

‡ Liegt der KoCoBox MED+ im Auslieferungskarton bei.

× Nur zur internen Verwendung, wird nicht an Endkunden ausgeliefert.

Tabelle 1.7.: 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 1: Anforderungen an den Netzkonnektor*“ [BSI-CC-PP-0097]

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.5	Resistenz gegen Angriffspotential „High“
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-0097]. 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-0097] gefordert werden.

TOE Typ Das Schutzprofil fordert, dass der TOE ein *Produkt* ist, das die „Sicherheitsfunktionalität einer Firewall, eines VPN-Clients sowie von Servern für einen Zeitdienst, einen Namensdienst (DNS) und einen DHCP-Dienst“ umfasst. Zudem beinhaltet es die Basisfunktionen zum Aufbau von TLS-Kanälen zu anderen IT-Produkten. Der TOE, der in diesem Security Target beschrieben wird, ist ein solches Produkt. Es wird auch mit dem Begriff *Netzkonnektor* bezeichnet.

Definition des Sicherheitsproblems Die Definition des Sicherheitsproblems, d. h. die Bedrohungen, Annahmen und die organisatorischen Sicherheitspolitiken sind direkt aus dem Schutzprofil [BSI-CC-PP-0097] übernommen.

Sicherheitsziele und Sicherheitsanforderungen Die Sicherheitsziele und Sicherheitsanforderungen sind dem Schutzprofil [BSI-CC-PP-0097] 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.

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. Für die Funktionalität „Laufzeitverlängerung“ gemäß *Feature Laufzeitverlängerung gSMC-K* kommen die vom TSP verlängerten AUT-Zertifikate der gSMC-K hinzu. Für diese Zertifikate muss kein neuer Wert eingeführt werden, sie werden durch die bestehenden Werte „Management-Daten bei Übertragung, bzw. Speicherung“ subsumiert. Für sie gelten die Schutzziele Integrität und – bei der Übertragung – Authentizität [gemF_LZV_gSMC-K].

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 [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

Die in [BSI-CC-PP-0097] und in den [BSI-CC-PP-0098] aufgelisteten und angenommenen *Organisatorische Sicherheitspolitiken* gelten bezüglich des TOE Scopes ohne Anpassung, vgl. hierzu auch die

Anmerkungen im Vorwort dieses Security Targets.

OSP.AK.Fachanwendungen

Die Fachanwendungen der TI und zentrale Dienste der TI-Plattform sind vertrauenswürdig und verhalten sich entsprechend ihrer Spezifikation. Der Konnektor unterstützt den Fachdienst Versichertenstammdatenmanagement**, die Fachanwendung ePA** und die Kommunikation mit dem zentralen Verzeichnisdienst. Fachdienste und Fachmodule kommunizieren über gesicherte Kanäle. Für zentrale Dienste der TI kann eine geschützte Kommunikation bereit gestellt werden. Durch Fachanwendungen genutztes Schlüsselmaterial wird wirksam vor Angriffen geschützt. Wird dennoch eine Komponente einer Fachanwendung und/oder sein Schlüsselmaterial erfolgreich angegriffen, so werden die betroffenen Schlüssel zeitnah gesperrt.

3.4. Annahmen

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.

A.NK.AK und A.NK.CS

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 Unterabschnitt 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 [ALC_DEL] beschrieben. Das Administratorhandbuch listet in Abschnitt 4.2 die Art und die Platzierung der verschiedenen Siegel auf dem Gehäuse des Konnektors auf [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*, *Supporter* etc., vgl. [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 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.

4.3. Erklärung der Sicherheitsziele des Netzkonnektors

4.3.1. 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.

4.3.1.1. Abwehr der Bedrohungen durch die Sicherheitsziele

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

4.3.1.2. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

Die Abbildungen der organisatorischen Sicherheitspolitiken auf Sicherheitsziele wird unverändert aus dem Schutzprofil übernommen.

4.3.1.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Die Abbildung der Annahmen auf Sicherheitsziele der Umgebung wird 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

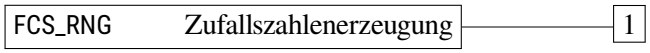
5. Definition der erweiterten Komponenten

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 legt das Schutzprofil in einem Anwendungshinweis zu diesem Sicherheitsziel nahe, 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. Die vom Konnektor verwendeten gSMC-K bieten Zufallsgeneratoren der Klassen PTG.2 (Hersteller G&D, [STARCOS-ST_36; STARCOS-ST_37]), bzw. PTG.3 (Hersteller T-Systems, [TCOS-ST]) an.

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] 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-0097] zu entnehmen. Bei Sicherheitsanforderungen, die durch das Security Target hinzugefügt werden, sind die Hierarchie- und Abhängigkeitsinformationen aufgeführt.

6.1.1. Hinweise zur Notation

Harmonisierung der Schutzprofile

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.

Hervorhebungen der Operationen

Die Prüfvorschrift „Konnektor“ verlangt vom Hersteller, dass die Abdeckung der Anforderungen, die nicht durch das Schutzprofil erklärt sind, im Security Target dokumentiert wird. In den allermeisten Fällen führen diese herstellerspezifischen Erweiterungen zu Operationen an SFR oder zur Einführung neuer SFR, die das Schutzprofil nicht vorsieht. In diesem Schutzprofil sind zwei Klassen von Operationen farblich unterschiedlich markiert. Operationen, die der Hersteller vornimmt, weil das Schutzprofil sie fordert oder die der Hersteller vornimmt, um den TOE gegenüber dem Schutzprofil zu verfeinern, sind blau markiert. Operationen, die der Hersteller vorgenommen hat, weil die Prüfvorschrift „Konnektor“ dies verlangt, sind grün markiert. Tabelle 6.1 zeigt, wie sich dies auf die Formatierung der einzelnen Operationen auswirkt.

Dieses Vorgehen dient ausschließlich der Steigerung der Lesbarkeit. Aus Sicht der Common Criteria Zertifizierung gibt es keinen semantischen Unterschied zwischen einer blau und einer grün gekennzeichneten Operation.

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Die Modellierungen des Schutzprofils [BSI-CC-PP-0097] gelten auch für dieses Security Target. Für die Funktionalität „Laufzeitverlängerung“ gemäß *Feature Laufzeitverlängerung gSMC-K* wird ein weiteres Objekt hinzugefügt [gemF_LZV_gSMC-K], vgl. Tabelle 6.2.

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 und unterstrichen gesetzt.
	Auswahl (Selection)	Auswahlen sind *in blauer Schrift, kursiv unterstrichen* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **in blauer Schrift und fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**in blauer Schrift, fett und durchgestrichen**~~ gesetzt.
Spec.	Zuweisung (Assignment)	Zuweisungen sind in grüner Schrift und unterstrichen gesetzt.
	Auswahl (Selection)	Auswahlen sind *in grüner Schrift, kursiv unterstrichen* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **in grüner Schrift und fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**in grüner Schrift, fett und durchgestrichen**~~ gesetzt.

Tabelle 6.1.: Typographische Konventionen

Objekt	Beschreibung	Sicherheitsattribut	
O_Zertifikat_gSMC-K	Vom TSP in der Laufzeit verlängerte Zertifikate einer gSMC-K. Umfasst die Zertifikate C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS	Identität: Integ. und Auth.:	ICCSN, öffentlicher Schlüssel, Ablaufdatum, Signatur

Tabelle 6.2.: Objekte des TOE

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 — The TSF shall provide a communication channel between itself and another trusted IT product **VPN-Konzentrator der Telematikinfrastruktur**[1] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[2] and protection of the channel data from modification **and**[3] disclosure.

FTP_ITC.1.2/NK.VPN_TI — The TSF shall permit *the TSF*[4] to initiate communication via the trusted channel.

[1] Refinement
[2] Refinement
[3] Refinement: *or* → *and*
[4] Selection: *the TSF, another trusted IT product*

FTP_ITC.1.3/NK.VPN_TI — The TSF shall initiate communication via the trusted channel for communication with the TI[5].

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

FTP_ITC.1.1/NK.VPN_SIS — The TSF shall provide a communication channel between itself and another trusted IT product **Sicherer Internet Service (SIS)**[6] that is logically distinct from other communication channels and provides assured identification of its end points **using certificate based authentication**[7] and protection of the channel data from modification **and**[8] disclosure.

FTP_ITC.1.2/NK.VPN_SIS — The TSF shall permit *the TSF*[9] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.VPN_SIS — The TSF shall initiate communication via the trusted channel for all communication with the SIS[10].

6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung

FDP_IFC.1/NK.PF
Subset information flow control

FDP_IFC.1.1/NK.PF — The TSF shall enforce the packet filtering SFP (PF SFP)[11] on the subjects

(1) IAG,
(2) VPN concentrator of the TI,
(3) VPN concentrator of the SIS,
(4) the TI services,
(5) application connector (except the service modules),
(6) the service modules (German: Fachmodule) running on the application connector,
(7) active entity in the LAN,
(8) CRL download server,
(9) hash & URL server,
(10) registration server of the VPN network provider,

[5] Assignment: *list of functions for which a trusted channel is required*
[6] Refinement
[7] Refinement
[8] Refinement: *or* → *and*
[9] Selection: *the TSF, another trusted IT product*
[10] Assignment: *list of functions for which a trusted channel is required*
[11] Assignment: *information flow control SFP*

(11) ~~remote management server,~~[12]

(12) TSL-Download-Punkt des TSL-Dienstes[13]

the information

(1) incoming information flows

(2) outgoing information flows

and the operation

(1) receiving data,

(2) sending data,

(3) communicate (i.e. sending and receiving data)[14].

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

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

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

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

[12] Deletion: *Vgl. ST-Anwendungshinweis 11 zu FTP_TRP.1/NK.Admin*

[13] Refinement: *Gemäß Vorgaben aus TIP1-A_4736-02*

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

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

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

a) by means of IPSEC protocol with VPN concentrator of TI with IP-Address VPN_KONZENTRATOR_TI_IP_ADRESS,

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

c) by means of protocols HTTP and HTTPS with IP-Address CERT_CRL_DOWNLOAD_ADDRESS, DNS_ROOT_ANCHOR_URL, hash & URL Server, registration server and ~~remote management server~~[15] **TSL-Download-Punkt des TSL-Dienstes**[16],

d) by means of protocol DNS to any destination.

(5) The active entities in the LAN with IP addresses within ANLW_LAN_NETWORK_SEGMENT or ANLW_LEKTR_INTRANET_ROUTES are allowed to communicate with the connector for access to base services.

(6) The application connector is allowed to communicate with active entities in the LAN.

(7) The TSF shall allow

a) to establish the IPsec tunnel with the VPN concentrator of TI if initiated by the application connector and

b) to send packets with destination IP address VPN_KONZENTRATOR_TI_IP_ADDRESS and to receive packets with source IP address VPN_KONZENTRATOR_TI_IP_ADDRESS in the outer header of the IPsec packets.

(8) The following rules based on the IP addresses in the inner header of the IPSec packet apply for the communication TI through the VPN tunnel between the connector and the VPN concentrator:

a) Communication is allowed between entities with IP address within NET_TI_ZENTRAL and application connector.

[15] Deletion: *Vgl. ST-Anwendungshinweis 11 zu FTP_TRP.1/NK.Admin*
[16] Refinement: *Gemäß Vorgaben aus TIP1-A_4736-02*

b) Communication is allowed between entities with IP address within NET_TI_GESICHERTE_FD and application connector.

c) If MGM_LU_ONLINE=Enabled the communication between entities with IP address within NET_TI_GESICHERTE_FD and by service moduls is allowed.

d) Communication between entities with IP address within NET_TI_OFFENE_FD and active entity in the LAN is allowed.

e) Communication between entities with IP address within NET_TI_OFFENE_FD and a service module is allowed.

f) If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled) the TSF shall allow communication of connector with DNS with IP address within DNS_SERVERS_BESTANDSNETZE.

g) If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled) the TSF shall allow communication of active entities in the LAN with entities with IP address within ANLW_AKTIVE_BESTANDSNETZE.

(9) The TSF shall allow

a) to establish the IPsec tunnel with the SIS concentrator if initiated by the application connector and

b) to send packets with destination IP address VPN_KONZENTRATOR_SIS_IP_ADDRESS and to receive packets with source IP address VPN_KONZENTRATOR_SIS_IP_ADDRESS in the outer header of the IPsec packets..

(10) Packets with source IP address within NET_SIS shall be received with outer header of the VPN tunnel from the VPN concentrator of the SIS only.

(11) For the communication though the VPN tunnel with VPN concentrator of the SIS the following rules based on the IP addresses in the inner header of the IPSec packets apply:

a) If (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=SIS) the application connector and active entities in the LAN are allowed to communicate through the VPN tunnel with the SIS.

b) The rules ANLW_FW_SIS_ADMIN_RULES applies if defined.

(12) The TSF shall redirect the packets received from active entities in the LAN to the default gateway if the packet destination address is not (NET_TI_ZENTRAL or NET_TI_OFFENE_FD or NET_TI_GESICHERTE_FD or ANLW_AKTIVE_BESTANDSNETZE) and if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=IAG).

(13) The TSF shall redirect communication from IAG to active entities in the LAN if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS=IAG und ANLW_IAG_ADDRESS≠““).[17]

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

The TSF shall enforce the following additional information flow control SFP rules:

(1) The TSF shall enforce SFP rules ANLW_FW_SIS_ADMIN_RULES

(2) The TSF shall transmit data (except for establishment of VPN connections) to the WAN only if the IPsec VPN tunnel between the TSF and the remote VPN concentrator has been successfully established and is active and working[18].

FDP_IFF.1.4/NK.PF

The TSF shall explicitly authorise an information flow based on the following rules: Stateful Packet Inspection, none[19].

FDP_IFF.1.5/NK.PF

The TSF shall explicitly deny an information flow based on the following rules:

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

[18] Assignment: *additional information flow control SFP rules*

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

(1) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with NET_TI_GESICHERTE_FD, NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL outside VPN channel to VPN concentrator of the TI.

(2) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with SIS outside VPN channel to VPN concentrator of the SIS.

(3) The TSF prevents communication of active entities in the LAN with destination IP address within ANLW_AKTIVE_BESTANDSNETZE initiated by active entities in the LAN, if (MGM_LOGICAL_SEPARATION=Enabled).

(4) The TSF prevents communication of active entities in the LAN with entities with IP addresses within ANLW_BESTANDSNETZE but outside ANLW_AKTIVE_BESTANDSNETZE.

(5) The TSF prevents communication of service modules with NET_TI_ZENTRAL, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE and internet via SIS or IAG.

(6) The TSF prevents communication initiated by entities with IP address within NET_TI_GESICHERTE_FD, NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL (except the connector itself), ANLW_BESTANDSNETZE and NET_SIS.

(7) The TSF prevents communication of entities with IP addresses in the inner header within NET_TI_ZENTRAL, NET_TI_GESICHERTE_FD, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE, ANLW_LAN_ADDRESS_SEGMENT, ANLW_LEKTR_INTRANET_ROUTES and ANLW_WAN_NETWORK_SEGMENT coming through the VPN tunnel with VPN concentrator of the SIS.

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

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

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.[20]

ST-Anwendungshinweis 2

Die [gemSpec_Kon] gibt sämtliche Paketfilterregeln vor. Damit sind auch die erlaubten Protokolle durch TIP1-A_4747 [gemSpec_Kon] 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 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

The TSF shall enforce the PF SFP[21] to provide *restrictive*[22] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/NK.PF

The TSF shall allow ~~the~~[23] nobody[24] to specify alternative initial values to override the default values when an object or information is created.

[20] Assignment: *Additional rules, based on security attributes, that explicitly deny information flows*
[21] Assignment: *access control SFP, information flow control SFP*
[22] Selection: *choose one of: restrictive, permissive, [assignment: other property]*
[23] Deletion: *Editorielle Anpassung*
[24] Assignment: *the authorised identified roles*

6.2.3. Netzdienste

FPT_STM.1/NK
Reliable time stamps

FPT_STM.1.1/NK	The TSF shall be able to provide reliable time stamps.
Refinement:	Die Zuverlässigkeit (reliable) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls 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*[25] 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 TIP1-A_4843 [gemSpec_Kon]. Der Netzkonnektor steuert das Display über die logische Schnittstelle LS.DISPLAY an.
ST-Anwendungshinweis 5	Das Schutzprofil fordert in Anwendungshinweis 72, 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 Application 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	The TSF shall provide the capability to consistently interpret information – distributed in the form of a TSL (Trust-Service Status List) and CRL (Certificate Revocation List) information – about the validity of certificates and about the domain (Telematikinfrastruktur) to which the VPN concentrator with a given certificate connects[26] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/NK.Zert	The TSF shall use interpretation rules[27] when interpreting the TSF data from another trusted IT product.

[25] Selection: *nicht mehr als 330ms, [Zuweisung: andere Zeit]*
[26] Assignment: *list of TSF data types*
[27] Assignment: *list of interpretation rules to be applied by the TSF*

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].

Additional interpretation rules for the *TSL detached signature* have to be applied upon TSL download from the internet.[28]

ST-Anwendungshinweis 6

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.

ST-Anwendungshinweis 7

Der Konnektor unterstützt einen Wechsel des Vertrauensraumes (ECC-Migration) von RSA nach ECC-RSA mit Hilfe von Cross-Zertifikaten gemäß A_17821 [gemSpec_PKI, Abschnitt 8.1.2] und A_17837-01 [gemSpec_Kon]. Der Wechsel des Vertrauensraums kann automatisch beim Bootup A_20469-02 oder manuell A_17345 durchgeführt werden.

Bis zum vollständigen Abschluss der ECC-Migration werden zwei TSL-Varianten (TSL [RSA] und TSL [ECC-RSA]) vom TSL-Dienst bereitgestellt und vom Konnektor entsprechend dem etablierten Vertrauensraum verwendet [gemSpec_PKI, Abschnitt 8.1.1].

ST-Anwendungshinweis 8

Für den alternativen TSL Download aus dem Internet sieht die Spezifikation den Download einer weiteren TSL Signatur vor, die vor dem Import der TSL geprüft werden muss. Die Interpretationsregeln sind in A_21185 spezifiziert.

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[29].

[28] Refinement: *Gemäß Vorgaben aus A_21185*

[29] Assignment: *list of objects*

Refinement:	Die sensitiven Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. Reset, überschrieben werden. **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*[30] to demonstrate the correct operation of *stored TSF executable code*[31].
FPT_TST.1.2/NK	The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[32].
FPT_TST.1.3/NK	The TSF shall provide authorised users with the capability to verify the integrity of *stored TSF executable code*[33].
ST-Anwendungshinweis 9	The „stored TSF executable code“ comprises not only strictly the code, but all parts of the firmware such as XML schema files.

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)[34] in excess of limits that ensure that no leakage of this sensitive data occurs[35] 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*[36],

(3) *key material used to verify the integrity and authenticity of software updates*[37],

(4) *none*[38],

[30] 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]*
[31] Selection: *[assignment: parts of TSF], the TSF*
[32] Selection: *[assignment: parts of TSF data], TSF data*
[33] Selection: *[assignment: parts of TSF], the TSF*
[34] Assignment: *types of emissions*
[35] Assignment: *specified units*
[36] Selection: *none, key material used to verify the TOE's integrity during self tests*
[37] Selection: *none, key material used to verify the integrity and authenticity of software updates*
[38] Selection: *none, key material used to decrypt encrypted software updates (if applicable)*

(5) *key material used for authentication of administrative users*[39],

(6) none[40] and

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

(8) none[41].

FPT_EMS.1.2/NK

The TSF shall ensure attackers on the transport network (WAN) or on the local network (LAN)[42] are unable to use the following interface WAN interface or LAN interface of the connector[43] to gain access to **the sensitive data (TSF data and user data) listed above**[44].

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-0097]**

b) All auditable events for the *not specified*[45] level of audit; and

c)
- start-up, shut down and reset (if applicable) of the TOE
- VPN connection to TI successfully / not successfully established,
- VPN connection to SIS successfully / not successfully established,
- TOE cannot reach services of the transport network,
- IP addresses of the TOE are undefined or wrong,
- TOE could not perform system time 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[46]

FAU_GEN.1.2/NK.SecLog

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

[39] Selection: *none, key material used for authentication of administrative users (if applicable)*
[40] Assignment: *list of other types of TSF data (may be empty)*
[41] Assignment: *list of types of user data (may be empty)*
[42] Assignment: *type of users*
[43] Assignment: *type of connection*
[44] Refinement: *refinement (Umformulierung) sowie Zuweisung der beiden assignments: [assignment: list of types of TSF data] and [assignment: list of types of user data]*
[45] Selection: *choose one of: minimum, basic, detailed, not specified*
[46] Assignment: *other specifically defined auditable events*

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[47].

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 10

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

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

6.2.6. Administration

FMT_SMR.1/NK
Security roles

FMT_SMR.1.1/NK

The TSF shall maintain the roles

- Administrator,
- SIS,
- TI
- Anwendungskonnektor[48].

FMT_SMR.1.2/NK

The TSF shall be able to associate users with roles.

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*[49] the real time clock, packet filtering rules and other TSF data named in the „Object" column of the following table[50] to the role Administrator.

[47] Assignment: *other audit relevant information*
[48] Assignment: *the authorised identified roles*
[49] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[50] Assignment: *list of other TSF data (may be empty)*

Operation	Object
Modify	System time[51]
Create, Modify, Delete	Packet filtering rules
Perform	Self-tests
Perform	Software update
Perform	Activation and deactivation of VPN connections[52]
Import	Certificate C.NK.VPN with extended validity.

FIA_UID.1/NK.SMR
Timing of identification

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

- all actions except for administrative actions (as specified by FMT_SMF.1/NK, see below)[53]

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

FIA_UID.1.2/NK.SMR — The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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*[54] 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*[55].

FTP_TRP.1.2/NK.Admin — The TSF shall permit *local users*[56] to initiate communication via the trusted path.

FTP_TRP.1.3/NK.Admin — The TSF shall require the use of the trusted path for *initial user authentication and administrative actions.*[57]

[51] Only available in offline mode, when there is no connection to the NTP servers.
[52] 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.
[53] Assignment: *list of TSF-mediated actions*
[54] Selection: *remote, local*
[55] Selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*
[56] Selection: *the TSF, local users, remote users*
[57] Selection: *initial user authentication, [assignment: other services for which trusted path is required]*

ST-Anwendungshinweis 11 Der TOE setzt die Funktionalität für das Remote Management nicht um.

FMT_SMF.1/NK
Specification of Management Functions

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

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

  (Verwalten der Filterregeln für den dynamischen Paketfilter.)
- Management of TLS-Connections (as required for FMT_MOF.1/NK.TLS).

  (Verwalten der Anwendungskonnektor.)[58]

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*[59] the security attributes packet filtering rules to the roles „Administrator“, no other role[60].

The refinement from [BSI-CC-PP-0097] applies without modification.

ST-Anwendungshinweis 12 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 The TSF shall use the following rules to set the value of security attributes:

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

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

[58] Assignment: *list of management functions to be provided by the TSF*
[59] Selection: *query, modify, delete, [assignment: other operations]*
[60] Assignment: *(may be empty): other authorised identified roles*

Wenn die Authentisierung des Administrators in der IT-Einsatzumgebung erfolgt und nicht erfolgreich durchgeführt werden konnte, dann übernehmen die TSF diesen Status und weisen dem Sicherheitsattribut „Autorisierungsstatus“ des auf diese Weise nicht authentisierten Benutzers „Administrator“ den Wert „nicht autorisiert“ zu.[61]

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

Refinement:

Der Hash-Algorithmus SHA-1 ist im Kontext IPsec ausschließlich für das hash & URL-Verfahren zulässig.

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-256, no other[63] and cryptographic key sizes 256 bit[64] that meet the following: FIPS PUB 180-4 [FIPS 180-4], RFC 4868 [RFC 4868], RFC 7296 [RFC 7296].

FCS_COP.1/NK.Auth
Cryptographic operation

FCS_COP.1.1/NK.Auth

The TSF shall perform

a) verification of digital signatures and

b) signature creation with support of gSMC-K storing the signing key and performing the RSA **and ECDSA**[65] operations[66]

in accordance with a specified cryptographic algorithm sha256withRSAEncryption OID 1.2.840.113549.1.1.11 **, ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 with curves brainpoolP256r1**[67] and

[61] Assignment: *rules for setting the values of security attributes*
[62] Assignment: *list of SHA-2 Algorithms with more than 256 bit size*
[63] Assignment: *list of SHA-2 Algorithms with more than 256 bit size*
[64] Assignment: *cryptographic key sizes*
[65] Refinement: *Gemäß Vorgaben aus A_17125*
[66] Assignment: *list of cryptographic operations*
[67] Assignment: *cryptographic algorithm*

cryptographic key sizes 2048 bit **or 256 bit for ECDSA**[68] that meet the following: RFC 8017 (PKCS#1) [RFC 8017], FIPS PUB 180-4 [FIPS 180-4]**, RFC 5639 [RFC 5639], FIPS PUB 186-4 [FIPS 186-4]**.[69]

ST-Anwendungshinweis 13 — Die TSF zur Erstellung von ECDSA-Signaturen mit Unterstützung der gSMC-K werden nur dann umgesetzt, wenn die Einsatzumgebung in Form der gSMC-K ECC-Schlüsselmaterial bereitstellt, siehe Unterabschnitt 1.4.3.

FCS_COP.1/NK.ESP
Cryptographic operation

FCS_COP.1.1/NK.ESP — The TSF shall perform symmetric encryption and decryption with Encapsulating Security Payload[70] in accordance with a specified cryptographic algorithm AES-CBC (OID 2.16.840.1.101.3.4.1.42) **or AES-GCM**[71] and cryptographic key sizes 256 bit **for AES-CBC or 128, 256 bit for AES-GCM**[72] that meet the following: FIPS PUB 197 [FIPS 197], RFC 3602 [RFC 3602], RFC 4303 (ESP) [RFC 4303], specification [gemSpec_Krypt]**, RFC 5282 [RFC 5282], RFC 4106 [RFC 4106]**[73].

FCS_COP.1/NK.IPsec
Cryptographic operation

FCS_COP.1.1/NK.IPsec — The TSF shall perform VPN communication[74] in accordance with a specified cryptographic algorithm IPsec-protocol **with AES-CBC or AES-GCM**[75] and cryptographic key sizes 256 bit **for AES-CBC or 128, 256 bit for AES-GCM**[76] that meet the following: RFC 4301 (IPsec) [RFC 4301], specification [gemSpec_Krypt]**, RFC 5282 [RFC 5282]**[77].

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-SHA256[78] and specified cryptographic key sizes 256 bit[79] that

[68] Assignment: *cryptographic key sizes*
[69] Assignment: *list of standards*
[70] Assignment: *list of cryptographic operations*
[71] Assignment: *cryptographic algorithm*
[72] Assignment: *cryptographic key sizes*
[73] Assignment: *list of standards*
[74] Assignment: *list of cryptographic operations*
[75] Assignment: *cryptographic algorithm*
[76] Assignment: *cryptographic key sizes*
[77] Assignment: *list of standards*
[78] Assignment: *cryptographic key generation algorithm*
[79] Assignment: *cryptographic key sizes*

meet the following: specification [gemSpec_Krypt], TR-03116 [TR-03116-1].

FCS_CKM.2/NK.IKE
Cryptographic key distribution

FCS_CKM.2.1/NK.IKE

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method IPsec IKE v2 that meets the following standard: RFC 7296 [RFC 7296], specifications [gemSpec_Krypt], TR-02102-3 [TR-02102-3].

The following sets of algorithms and configurations is supported for IKEv2 connections, with ECC based algorithms chosen preferably:

ECC based (preferred):

- **ECDH Curve brainpoolP256r1**
- **Forward secrecy: yes**
- **Authenticated Encryption: AEAD-AES-128-GCM, AEAD-AES-256-GCM, AEAD-AES-128-GCM-12, AEAD-AES-256-GCM-12**
- **PRF: PRF-HMAC-SHA-256**
- **Peer authentication: X.509 certificate with ECDSA 256 bit keys based on brainpoolP256r1.**

RSA based:

- **Diffie-Hellman Group 14**
- **DH exponent minimum length: 384 bits**
- **Forward secrecy: yes**
- **Encryption: AES-256-CBC**
- **Authentication: HMAC-SHA-256-128**
- **PRF: PRF-HMAC-SHA-256**
- **Peer authentication: X.509 certificate with RSA 2048 bit keys**

In both sets, IKE lifetime limited to 161 hours, IPsec SA lifetime limited to 23 hours. Rekeying will occur after that.

ST-Anwendungshinweis 14

Die Erläuterungen aus ST-Anwendungshinweis 13 gelten ebenfalls für dieses SFR.

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 constant values[80] that meets the following: none[81].

[80] Assignment: *cryptographic key destruction method*
[81] Assignment: *list of standards*

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 — The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and **is able to**[82] provide**s** assured identification of its end points and protection of the channel data from modification **and**[83] disclosure.

FTP_ITC.1.2/NK.TLS — The TSF **must be able to**[84] permit *the TSF or another trusted IT-Product*[85] to initiate communication via the trusted channel.

FTP_ITC.1.3/NK.TLS — The TSF shall initiate communication via the trusted channel for communication required by the Anwendungskonnektor, any connection specified in Table B.5.[86]

Refinement: Das Refinement im Schutzprofil [BSI-CC-PP-0097] gilt ohne Einschränkungen. Die umgesetzten Cipher Suiten aus dem Schutzprofil und der gematik Spezifikation [gemSpec_Krypt] werden in Tabelle B.1 auf Seite 88 wiederholt.

Zusätzlich zu den im Schutzprofil geforderten Cipher Suiten unterstützt der TOE die ECDSA-basierten Suiten:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Diese Cipher Suiten werden, wenn der TOE als Client agiert, in der *Client Hello*-Nachricht als erste gesendet. Der TOE fordert damit den Peer auf, vorzugsweise eine dieser beiden Suiten zu verwenden. Der TOE unterstützt ausschließlich die im Schutzprofil genannten und hier ergänzten Cipher Suiten. Andere Cipher Suiten können nicht verwendet werden.

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)

[82] Refinement: *dieses Refinement soll darauf hinweisen, dass der Netzkonnektor die Möglichkeit implementiert, beide Seiten zu authentisieren, dass es aber Entscheidung des nutzenden Systems (i.a. der Anwendungskonnektor) ist, inwieweit diese Authentisierung genutzt wird.*
[83] Refinement: *or → and*
[84] Refinement: *shall → must be able to*
[85] Selection: *the TSF, another trusted IT-Product*
[86] Assignment: *list of other functions for which a trusted channel is required*

(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) importierte X.509 Zertifikate und deren private Schlüssel für Konnektorauthentisierung.[87]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/NK.TLS.Zert — The TSF shall use interpretation rules[88] when interpreting the TSF data from another trusted IT product.

(1) Die Interpretationsregeln werden in TUC_PKI_018 „Zertifikatsprüfung in der TI“ [gemSpec_PKI, Abschnitt 8.3.1.1] definiert. Die Parameter für Zertifikatsprüfung werden in GS-A_4663 spezifiziert. [gemSpec_PKI, Abschnitt 8.4.1].[89]

(2) Die ggf. zu prüfenden zulässigen Rollen werden in GS-A_4446-05 [gemSpec_OID] aufgeführt. Tabelle B.5 listet in der Spalte „Identität des Peer“ die für die jeweilige Verbindung relevante Rolle auf.[90]

(3) Darüberhinaus definiert GS-A_5215 Regeln für die Interpretation von Zeitstempeln, die in OCSP-Responses eingebettet sind [gemSpec_PKI, Abschnitt 9.1.2.2].[91]

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

FCS_CKM.1.1/NK.TLS — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384[92]

and specified cryptographic key sizes 128 bit for AES-128, 256 bit for AES-256, 160 for HMAC with SHA, 256 for HMAC with

[87] Assignment: *additional list of data types*
[88] Assignment: *list of interpretation rules to be applied by the TSF*
[89] Refinement: *Präzisierung der Interpretationsregeln*
[90] Refinement: *Ergänzt gemäß Prüfaufgabe „Rollenprüfung bei TLS“ aus [TR-03157]*
[91] Refinement: *Gemäß Vorgaben aus GS-A_5215*
[92] Refinement: *Gemäß Vorgaben aus A_17094-01, A_17124-01*

SHA-256 and 384 for HMAC with SHA-384 that meet the following: Standard RFC 5246 [RFC 5246], **RFC 3526 [RFC 3526]**[93]**, RFC 5639 [RFC 5639], RFC 7027 [RFC 7027]**[94].

Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves according to FIPS PUB 186-4 [FIPS 186-4] as well as the brainpoolP256r1 and the brainpoolP384r1 curves according to RFC 5639 and RFC 7027.[95]

Ephemeral DH key exchange supports only Diffie-Hellman Group 14. The DH exponent shall have a minimum length of 384 bits. Forward secrecy shall be provided.[96]

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

FCS_COP.1.1/NK.TLS.HMAC — The TSF shall perform HMAC value generation and verification[97] in accordance with a specified cryptographic algorithm HMAC with SHA-1, SHA-256 and SHA-384[98] and cryptographic key sizes 160 for HMAC with SHA, 256 for HMAC with SHA-256, and 384 for HMAC with SHA-384[99] that meet the following: Standards FIPS PUB 180-4 [FIPS 180-4] and RFC 2104 [RFC 2104][100].

FCS_COP.1/NK.TLS.AES
Cryptographic operation

FCS_COP.1.1/NK.TLS.AES — The TSF shall perform symmetric encryption and decryption[101] in accordance with a specified cryptographic algorithm AES-128 and AES-256 in CBC and GCM Mode[102] and cryptographic key sizes 128 bit for AES-128 and 256 bit for AES-256[103] that meet the following: FIPS PUB 197 [FIPS 197], NIST-SP800-38D [NIST SP 800-38D], RFC 5246 [RFC 5246], RFC 8422 [RFC 8422], RFC 5289 [RFC 5289], specification [gemSpec_Krypt][104].

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

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

[93] Refinement: *Gemäß Vorgaben aus GS-A_4384-01*
[94] Refinement: *Gemäß Vorgaben aus A_17094-01, A_17124-01*
[95] Refinement: *Gemäß Vorgaben aus GS-A_5345-01*
[96] Refinement: *Gemäß Vorgaben aus GS-A_4384-01*
[97] Assignment: *list of cryptographic operations*
[98] Assignment: *cryptographic algorithm*
[99] Assignment: *cryptographic key sizes*
[100] Assignment: *list of standards*
[101] Assignment: *list of cryptographic operations*
[102] Assignment: *cryptographic algorithm*
[103] Assignment: *cryptographic key sizes*
[104] Assignment: *list of standards*

a) verification of digital signatures and

b) signature creation with support of gSMC-K or SM-B storing the signing key and performing the RSA **and ECDSA**[105] operation**s and**

c) signature creation with signing keys either imported according to FDP_ITC.2/NK.TLS or self-created according to FCS_CKM.1/NK.Auth

in accordance with a specified cryptographic algorithm sha256withRSAEncryption OID 1.2.840.113549.1.1.11**, ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 with curves brainpoolP256r1**[106]**, secp256r1, secp384r1, brainpoolP384r1**[107] and cryptographic key sizes 2048 bit **to 8192 bit for RSA and 256 bit and 384 bit**[108] **for ECDSA**[109] **and hash algorithms SHA-256 and SHA-384**[110] that meet the following: RFC 8017 (PKCS#1) [RFC 8017], FIPS PUB 180-4 [FIPS 180-4]**, FIPS PUB 186-4 [FIPS 186-4], RFC 7027 [RFC 7027]**[111].

ST-Anwendungshinweis 15 Die Erläuterungen aus ST-Anwendungshinweis 13 gelten ebenfalls für dieses SFR.

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 ECC based on brainpoolP256r1 or secp256r1 curves and RSA[112] **with random number generator specified by FCS_RNG.1/Hash_DRBG** and specified cryptographic key sizes 2048 bit **and 3072 bit for RSA and 256 bit for ECC** that meet the following: Standard OID 1.2.840.113549.1.1.11, RFC 4055 [RFC 4055], BSI TR-03116-1 [TR-03116-1]**, BSI TR-03111 [TR-03111], RFC 5639 [RFC 5639], FIPS PUB 186-4 [FIPS 186-4]**.

The TSF shall

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

(2) create a PKCS#12 file [RFC 7292][113] **with the created certificate and the associated private key.**

[105] Refinement: *Gemäß Vorgaben aus A_17094-01*
[106] Refinement: *Gemäß Vorgaben aus GS-A_4357-02*
[107] Refinement: *Zusätzliche Kurven für Kompatibilität mit Browsern*
[108] Refinement: *Zusätzliche Schlüssellänge für Kompatibilität mit Browsern*
[109] Refinement: *Gemäß Vorgaben aus GS-A_4357-02*
[110] Refinement: *Gemäß Vorgaben aus A_21275-01*
[111] Refinement: *Gemäß Vorgaben aus A_17094-01*
[112] Assignment: *Algorithm for cryptographic key generation of key pairs*
Gemäß Vorgaben aus TIP1-A_4517-02, A_17124-01
[113] Refinement: *Die Quelle für den PKCS#12 Standard wurde gegenüber dem Schutzprofil aktualisiert.*

ST-Anwendungshinweis 16 — Die Erläuterungen aus ST-Anwendungshinweis 13 gelten ebenfalls für dieses SFR.

FCS_CKM.1/NK.Auth
Cryptographic key generation / TOE authentication

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 or FCS_COP.1] hier erfüllt durch FCS_COP.1/NK.TLS.Auth

FCS_CKM.4 hier füllt durch FCS_CKM.4/NK

FCS_CKM.1.1/NK.Auth — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA and ECC based on brainpoolP256r1, secp256r1 with random number generator specified by FCS_RNG.1/Hash_DRBG[114] and specified cryptographic key sizes 2048 bit and 3072 bit for RSA and 256 bit for ECC that meet the following: RFC 4055 [RFC 4055], BSI TR-03111 [TR-03111], RFC 5639 [RFC 5639], BSI TR-03116-1 [TR-03116-1], FIPS PUB 186-4 [FIPS 186-4].

The TSF shall

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

(2) create a PEM file with the created certificate.

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

FDP_ITC.2.1/NK.TLS — The TSF shall enforce the Certificate-Import-SFP[115] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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

[114] Assignment: *Algorithm for cryptographic key generation of key pairs, Gemäß Vorgaben aus A_21699-02*
[115] Assignment: *access control SFP(s) and/or information flow control SFP(s)*

(1) Die TSF importiert X.509 Zertifikate für Clientsysteme durch den Administrator über die Management-Schnittstelle.

(2) Die TSF importiert X.509 Zertifikate und deren private Schlüssel für Konnektorauthentisierung durch den Administrator über die Management-Schnittstelle.[116]

(3) Die TSF importiert im Rahmen der Laufzeitverlängerung X.509 Zertifikate (O_Zertifikat_gSMC-K) durch den Administrator über die Management-Schnittstelle oder durch einen Download von einem Downloadpunkt in der TI.[117]

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

FDP_ETC.2.1/NK.TLS — The TSF shall enforce the Certificate-Export-SFP[118] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/NK.TLS — The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/NK.TLS — The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/NK.TLS — The TSF shall enforce the following rules when user data is exported from the TOE:

(1) Die TSF exportiert X.509 Zertifikate für Clientsysteme und den zugehörigen privaten Schlüssel durch den Administrator über die Management-Schnittstelle. Als Exportformat wird PKCS#12 verwendet.

(2) Die TSF exportiert X.509 Zertifikate für Konnektorauthentisierung durch den Administrator über die Management-Schnittstelle. Als Exportformat wird PEM verwendet.[119]

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 function**s** 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:

[116] Assignment: *Gemäß Vorgaben aus A_21697-01*
[117] Assignment: *additional importation control rules, Gemäß Vorgaben aus A_21879, A_21749-03*
[118] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[119] Assignment: *additional exportation control rules, Gemäß Vorgaben aus A_21701*

(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) Which identity is used for TOE authentication:

- ID.AK.AUT from gSMC-K#2, or
- ID.AK.AUT with extended validity according to FDP_ITC.2.5/NK.TLS(3), or
- Identity from a self-generated certificate according to FCS_CKM.1/NK.Auth, or
- Identity from an imported certificate according to FDP_ITC.2.5/NK.TLS(2)

[120]

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 17 Gemäß A_18464 darf TLS 1.1 nicht mehr verwendet werden.

ST-Anwendungshinweis 18 TLS wird vom Konnektor von JSSE implementiert. Jeder in Java implementierte Teil des TOE kann prinzipiell eine TLS-Verbindung eröffnen. Es gibt keine Kontrollinstanz im System, die die Einhaltung

[120] Assignment: *additional rules, Gemäß Vorgaben aus A_21698, A_21702, A_21760-01*

der oben genannten Regeln einer TLS-Verbindung programmatisch erzwingt.

Die Parameter sind im Code fest verdrahtet und nicht vom Administrator manipulierbar. Ausnahmen hiervon: Die Punkte (9) und (10) in der Liste.

ST-Anwendungshinweis 19 — Der Administrator legt über die Management-Schnittstelle fest, welches Zertifikat verwendet wird. Der Anwendungskonnektor konfiguriert die TLS-Verbindungen TLS.2, TLS.3, TLS.4 und TLS.5 entsprechend dieser Festlegung.

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*[121] random number generator that implements: [122]

(1) If initialized with a random seed using PTRNG of class PTG.2 or PTG.3 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: [123]

(1) The RNG is initialized upon startup and repeatedly after 2048 requests with a random seed of minimally 384 bits using a PTRNG of class PTG.2 or PTG.3. The RNG generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability $w > 1 - 2^{(-16)}$.

[121] Selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*
[122] Assignment: *list of security capabilities*
[123] 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 20

FCS_RNG.1/Hash_DRBG is implemented by Hash_DRBG with SHA-256 according to NIST-SP800-90A [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.

The TOE environment provides different types of gSMC-K, depending on the hardware generation. G3 hardware exclusively uses STARCOS 3.6 cards that provide class PTG.2 RNG [STARCOS-ST_36]. G4 hardware uses either STARCOS 3.7 cards, that also provide PTG.2 RNG [STARCOS-ST_37], or TCOS cards, that provide random number generation of class PTG.3 [TCOS-ST].

FCS_COP.1/NK.SigVer

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.

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/NK.SigVer: The TSF shall perform signature verification[124] in accordance with a specified cryptographic algorithm according to Tabelle 6.3[125] and cryptographic key sizes according to Tabelle 6.3[126] that meet the following: PKCS#1 [RFC 8017], FIPS PUB 186-4 [FIPS 186-4], RFC 5639 [RFC 5639], FIPS PUB 180-4 [FIPS 180-4] and BSI TR-03111 [TR-03111, Section 5.2.2][127].

[124] Assignment: *list of cryptographic operations*
[125] Assignment: *cryptographic algorithm*
[126] Assignment: *cryptographic key sizes*
[127] Assignment: *list of standards*

Algorithm	Key size (bits)/Curve	Purpose: Verification of …
RSASSA-PSS w/ SHA256	2048	Signature of TSL, Signature of O_Zertifikat_gSMC-K
RSASSA-PSS w/ SHA256	2048 – 8192	Detached TSL signature
RSASSA-PSS w/ SHA512	2048	Firmware update signatures
RSASSA-PSS w/ SHA256	4096	Signatures during the firmware update process
RSASSA-PSS w/ SHA256/-384/-512	2048 – 8192	Signatures of OCSP-Responses and CRL
RSASSA-PKCS1-v1_5 w/ SHA256	2048	Signature of O_Zertifikat_gSMC-K
RSASSA-PKCS1-v1_5 w/ SHA256	2048 – 8192	Signatures of OCSP-Responses and CRL
RSASSA-PKCS1-v1_5 w/ SHA384	2048 – 8192	Signatures of OCSP-Responses and CRL
RSASSA-PKCS1-v1_5 w/ SHA512	2048 – 8192	Signatures of OCSP-Responses and CRL
ECDSA w/ SHA256	brainpoolP256r1	Signature of TSL, Detached TSL signature, Signature of O_Zertifikat_gSMC-K, Signatures of OCSP-Responses and CRL
ECDSA w/ SHA384	brainpoolP384r1	Signature of O_Zertifikat_gSMC-K, Signatures of OCSP-Responses and CRL
ECDSA w/ SHA512	brainpoolP512r1	Signature of O_Zertifikat_gSMC-K, Signatures of OCSP-Responses and CRL

Tabelle 6.3.: Algorithms, Key sizes/Curve and Purposes of Signature Verification for NK

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[128] in accordance with a specified cryptographic algorithm AES CBC with ESSIV[129] and cryptographic key sizes 256 bit[130] that meet the following: FIPS PUB 197 [FIPS 197], NIST-SP800-38A [NIST SP 800-38A], and ESSIV [ESSIV][131].

[128] Assignment: *list of cryptographic operations*
[129] Assignment: *cryptographic algorithm*
[130] Assignment: *cryptographic key sizes*
[131] Assignment: *list of standards*

6.3. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

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

6.3.1. Verfeinerung zur Vertrauenswürdigkeitskomponente ADV_ARC.1

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

6.3.2. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_OPE.1

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

6.3.3. Verfeinerung zur Vertrauenswürdigkeitskomponente ALC_DEL.1

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

6.4. Erklärung der Sicherheitsanforderungen

6.4.1. 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 in Tabelle 6.4 aufgeführt.

SFR	Abhängig von	Erfüllt durch
FCS_RNG.1/Hash_DRBG	Keine Abhängigkeiten	–
FCS_COP.1/NK.SigVer	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. Def. FCS_COP.1/NK.SigVer FCS_CKM.4/NK
FCS_COP.1/Storage.AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. Def. FCS_COP.1/Storage.AES FCS_CKM.4/NK
FCS_CKM.1/NK.Auth	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/NK.TLS.Auth FCS_CKM.4/NK

Tabelle 6.4.: Abhängigkeiten der hinzugefügten SFR des Netzkonnektors

6.4.2. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors

Das Schutzprofil zeigt die Abdeckung von Sicherheitszielen durch Sicherheitsanforderungen. Diese Abdeckung gilt auch in diesem Security Target.

Dieses Security Target fügt herstellereigene Sicherheitsanforderungen hinzu. Die neuen SFR werden ebenfalls bestehenden Sicherheitszielen zugeordnet. Tabelle 6.5 zeigt, welchen Sicherheitszielen die neuen SFR zugeordnet werden.

	O.NK.Admin_EVG	O.NK.EVG_Authenticity	O.NK.PF_LAN	O.NK.PF_WAN	O.NK.Protokoll	O.NK.Schutz	O.NK.Stateful	O.NK.TLS_Krypto	O.NK.VPN_Auth	O.NK.VPN_Integrität	O.NK.VPN_Vertraul	O.NK.Zeitdienst	O.NK.Zert_Prüf
FCS_CKM.1/NK.Auth	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/NK.SigVer	.	✓	.	.	.	✓	.	.	✓	.	.	.	.
FCS_COP.1/Storage.AES	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_RNG.1/Hash_DRBG	.	.	.	.	.	.	.	✓	.	.	.	.	.

Tabelle 6.5.: Abbildung der Sicherheitsziele des NK auf *eigene* Sicherheitsanforderungen

6.4.3. 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.

6.5. 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 Unterabschnitt 6.4.1.

FCS_COP.1/Storage.AES

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

FCS_COP.1/NK.SigVer

FCS_COP.1/NK.SigVer 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_CKM.1/NK.Auth

FCS_CKM.1/NK.Auth wurde hinzugefügt, um die Anforderung A_21699-02 zur Erstellung von Authentisierungszertifikaten für TLS-Verbindungen des Konnektors zu erfüllen. Die Modellierung der Abhän-

gigkeiten wurde aus dem vergleichbaren SFR FCS_CKM.1/NK.Zert übernommen.

6.6. Erklärung für die gewählte EAL-Stufe

Die Erklärung der gewählten EAL-Stufe wird unverändert aus dem Schutzprofil [BSI-CC-PP-0097] übernommen.

7. TOE Summary Specification

Dieses Kapitel vermittelt einen Überblick über die IT-Sicherheitsfunktionen des TOE, wie sie in der funktionalen Spezifikation beschrieben sind. Abschnitt 7.1 enthält Beschreibungen der allgemeinen technischen Verfahren, die der TOE anwendet, um die Sicherheitsanforderungen zu erfüllen. Abschnitt 7.2 zeigt die Beziehungen zwischen der Sicherheitsanforderungen aus Abschnitt 6.2 und den IT-Sicherheitsfunktionen aus Abschnitt 7.1.

7.1. TOE Sicherheitsfunktionen

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

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 diese 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 aufgebauten, noch zu einer im Aufbau befindlichen Verbindung gehören. Solche nichtwohlgeformeten 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 die Signatur separat im sicherern Datenspeicher in einer eigenen Signaturdatei abgespeichert wird. Für die Signatur wird ein privater Schlüssel der gSMC-K verwendet. Beim Systemstart werden alle Hashwerte neu berechnet und gegen die jeweilige Signatur geprüft. Zusätzlich werden die Pfade und Namen aller Daten- und Signaturdateien in einem Journal abgelegt und als Datei im sicheren Datenspeicher persistiert. 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 9 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 clientseitige Teil der 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.

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.

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 Prüfung von X.509-Identitäten und zur Verifikation von Signaturen. Die Funktionalität unterstützt die Signaturalgorithmen RSASSA-PKCS1-v1_5, RSASSA-PSS und ECDSA.

Die Schemata RSASSA-PSS und ECDSA werden auch zur Verifikation von Signaturen der TSL, der CRL und der OCSP-Responses verwendet (A_17205). Die Software Updates sind mit RSASSA-PSS signiert. Zusätzlich werden damit die Hashes des sicheren Datenspeichers und die Integrität der TSF geprüft. Die Hashes des sicheren Datenspeichers werden nicht vom TOE signiert, sondern von der gSMC-K in der Betriebsumgebung des Konnektors. Hashes und Zufallszahlen für diese Signaturen wiederum werden vom TOE generiert. 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.

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.

Umgesetzte SFR
FCS_COP.1/NK.Auth, FCS_COP.1/NK.SigVer

Der TOE verfolgt die Ablaufdaten kryptographischer Algorithmen. Die gematik spezifiziert diese Algorithmen und deren Ablaufdaten in GS-A_4357-02 (für nonQES) . Tabelle 7.1 listet die verschiedenen Algorithmen und deren Ablaufdaten gemäß der Spezifikation [gemSpec_Krypt] und den Vorgaben der SOG-IS Crypto Working Group. Für alle Jahreszahlen gilt der 31.12. als Stichtag. Der Hersteller ändert die Algorithmen und deren Ablaufdaten ausschließlich über Software-Updates. Der Administrator kann hieran keine Konfigurationsänderungen vornehmen. *Der TOE implementiert keine Funktionalität, die beim Ablauf der Algorithmen deren Verwendung einschränkt.* Dies gilt insbesondere für Signaturen auf Basis von 2048 Bit langen RSA-Schlüsseln. Das Ausphasen nicht mehr gewünschter Alogrithmen geschieht gemäß den Erläuterungen zu A_15590 „durch die Herausnahme der entsprechenden RSA-basierten Sub-CA-Zertifikate aus der TSL zum Zeitpunkt des Ablaufens der Zulässigkeit“ [gemSpec_Krypt, Abschnitt 2.1.1.1].

Algorithmus	Key Length	gematik	SOG-IS
RSASSA-PKCS1-v1_5	2048	2025	2025†
	>3000	–*	2027+‡
RSASSA-PSS	2048	–*	2025†
	>3000	–*	∞×
ECDSA	256	2029+	∞×

* GS-A_4357-02 macht zur Verwendung keine Aussage.
† *Legacy* mit Ablaufdatum wegen Schlüssellänge.
‡ *Legacy* ohne Ablaufdatum wegen Padding
× *Recommended* ohne Ablaufdatum

Tabelle 7.1.: Algorithmen für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen

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 oder ECDSA verwendet. Während des Schlüsselaustausches wird mit dem (Elliptic Curve) 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 oder durch die Nutzung von AEAD Konstruktionen 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.5 auf Seite 90. 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_COP.1/NK.TLS.HMAC
FPT_TDC.1/NK.TLS.Zert	FCS_COP.1/NK.TLS.AES
FCS_CKM.4/NK	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].

Im Fall einer zertifikatsbasierten Authentisierung kann der TOE X.509 Zertifikate für die Clientauthentisierung importieren oder selbst erzeugen und an den Benutzer ausliefern.

Der TOE setzt weiterhin die Anforderungen der gematik zur Behandlung von Authentisierungszertifikaten um. Standardmäßig verwendet der TOE das AUT-Zertifikat der gSMC-K#2, um sich gegenüber den Kommunikationspartnern zu authentifizieren. Alternativ dazu kann der TOE eigene Zertifikate generieren oder ein extern erzeugtes Zertifikat importieren. Beim Generieren bietet der TOE an, RSA- oder ECC-Zertifikate zu erstellen. Im Falle von ECC wählt der Administrator aus, ob Brainpool oder NIST zum Einsatz kommen. Über die Managementschnittstelle wählt der Administrator aus, welches dieses Zertifikat verwendet werden soll.

Umgesetzte SFR	
FCS_CKM.1/NK.Zert	FCS_CKM.1/NK.Auth
FDP_ITC.2/NK.TLS	FDP_ETC.2/NK.TLS

7.2. Verhältnis von SFR zu SF

Tabelle 7.2 zeigt, in welchem Verhältnis die im Abschnitt 6.2 definierten Sicherheitsanforderungen zu den in Abschnitt 7.1 beschriebenen Sicherheitsfunktionen des TOE stehen.

	SF.DynamicPacketFilter	SF.NetworkServices	SF.Administration/NK	SF.Audit/NK	SF.CryptographicServices/NK	SF.SelfProtection/NK	SF.VPN
FAU_GEN.1/NK.SecLog	.	.	.	✓	.	.	.
FAU_GEN.2/NK.SecLog	.	.	.	✓	.	.	.
FCS_CKM.1/NK.Auth	.	.	.	.	✓	.	.
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.SigVer	.	.	.	.	✓	.	.
FCS_COP.1/NK.TLS.AES	.	.	.	.	✓	.	.
FCS_COP.1/NK.TLS.Auth	.	.	.	.	✓	.	.
FCS_COP.1/NK.TLS.HMAC	.	.	.	.	✓	.	.
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	.	.	✓	.	.	.	.

Abbildung der SFR des NK auf Sicherheitsfunktionalitäten

	SF.DynamicPacketFilter	SF.NetworkServices	SF.Administration/NK	SF.Audit/NK	SF.CryptographicServices/NK	SF.SelfProtection/NK	SF.VPN
FPT_EMS.1/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 Sicherheitsfunktionalitäten

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
.	Leeres Feld, die Markierung dient als Lesehilfe
✓	Vom Schutzprofil vorgesehene Beziehung / vorgesehenes SFR
–	Nicht umgesetzte, vom Schutzprofil als optional vorgesehene Beziehung / vorgesehenes 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_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`	✓
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	`0xc0,0x2b`	✓
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	`0xc0,0x2c`	✓
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	`0x00,0x33`	✓
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	`0x00,0x39`	✓

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

Algorithmus	OID	Schlüssellänge
sha256withRSAEncryption	1.2.840.113549.1.1.11	2048 – 8192 bit
ecdsa-with-SHA256	1.2.840.10045.4.3.2	256 bit

Tabelle B.3.: Signaturalgorithmen 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.5 listet die Verbindungen auf, die der Konnektor eingeht. Die Spalten dieser Tabelle werden

in Tabelle B.4 beschrieben. Tabelle B.6 listet die Identität des TOE bei den TLS-Verbindungen auf, sofern die Identität eine Rolle spielt.

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.
Auth.	Gibt an, ob sich der TOE in dieser Verbindung authentifiziert. Die verwendeten Zertifikate sind in Tabelle B.6 gelistet.
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 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.4.: Legende zu den TLS Verbindungen

ID	Schnittstelle (Protokoll)	Rolle	Auth.*	Peer	Subsystem::Modul	Port	Identität des Peer	Authentifizierung des Peer durch
TLS.1	LS.LAN.HTTP_MGMT	Server	✓	Browser	Facade::Jetty-Configuration	9443	Benutzername/Passwort	AdminService::Core
TLS.2	LS.LAN.SOAP	Server	✓	Clientsystem	Facade::Jetty-Configuration	443	X.509 Zertifikate	*server_truststore.jks*
TLS.3	LS.LAN.SOAP	Server	✓	Clientsystem	Facade::Jetty-Configuration	443	HTTP Basic Authentication	AdminService::Core
TLS.4	LS.LAN.LDAP	Server	✓	Clientsystem	LDAPProxy::Core	636	X.509 Zertifikate	*server_truststore.jks*
TLS.5	LS.LAN.CETP	Client	✓	Clientsystem	SystemInformationService::Core	konfig.	X.509 Zertifikate	*server_truststore.jks*
TLS.6	LS.LAN.SICCT	Client	✓	eHealth Karten-terminal	CardService::de.ndesign.koco.ifd.sicct	4742	SMC-KT: ID.SMKT.AUT	CertificateService::Core
TLS.7	LS.WAN.RegService	Client	✓	Registrierungs-dienst	AdminService::RegistrationService	8443	C.ZD.TLS-S, 1.2.276.0.76.4.157	CertificateService::Core
TLS.8	LS.VPN_TI.LDAP	Client	.	Verzeichnis-dienst	LDAPProxy::Core	dyn.	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.	ID.ZD.TLS-S, 1.2.276.0.76.4.189	CertificateService::Core
TLS.10	LS.VPN_TI.VSDM	Client	✓	Intermediär VSDM	Fachmodule::VSDM_TLS	dyn.	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.	C.ZD.TLS-S, 1.2.276.0.76.4.160	CertificateService::Core
TLS.12	LS.VPN_TI.VAU	Client	.	ePA-Aktensystem	Kommunikationsdienste::VAU-Service	dyn.	C.FD.TLS-S, 1.2.276.0.76.4.206	CertificateService::Core
TLS.13	LS.VPN_TI.SGD	Client	.	SGD1/SGD2	Kommunikationsdienste::SGD-Service	dyn.	C.FD.TLS-S, 1.2.276.0.76.4.221	CertificateService::Core
TLS.14	LS.VPN_TI.Authn	Client	.	ePA-Authent.-dienst		dyn.	C.FD.TLS-S, 1.2.276.0.76.4.204	CertificateService::Core
TLS.15	LS.VPN_TI.Authz	Client	.	ePA-Autor.-dienst		dyn.	C.FD.TLS-S, 1.2.276.0.76.4.205	CertificateService::Core

* Für die verwendete Identität s. Tabelle B.6

Tabelle B.5.: TLS Verbindungen der KoCoBox MED+

Rolle	Verbindung	gSMC-K#2 / LZV		Generiert gemäß	Importiert gemäß	gSMC-K#2 / LZV		SMC-B	
		AK.AUT.R2048*	AK.AUT2.XXXX†	FCS_CKM.1/NK.Auth	FDP_ITC.2/NK.TLS	SAK.AUT.R2048	SAK.AUT2.XXXX‡	HCI.AUT.R2048	HCI.AUT.E256
Server	TLS.1	✓	✓	✓	✓	.	.	.	.
	TLS.2 / TLS.3	✓	✓	✓	✓	.	.	.	.
	TLS.4	✓	✓	✓	✓	.	.	.	.
Client	TLS.5	✓	✓	✓	✓	.	.	.	.
	TLS.6	.	.	.	.	✓	✓	.	.
	TLS.7	.	.	.	.	.	.	✓	✓
	TLS.10	.	.	.	.	.	.	✓	✓

* Browser verwenden üblicherweise EF.C.AK.AUT.R2048, da die gängigen Browser keine Brainpool-Kurven unterstützen.
† EF.C.AK.AUT2.XXXX nur bei dual-personalisierter gSMC-K#2.
‡ EF.C.SAK.AUT2.XXXX nur bei dual-personalisierter gSMC-K#2.

Tabelle B.6.: Identität des TOE bei TLS-Verbindungen

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 1.6.7. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. März 2023.

[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 1.6.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. März 2023.

[TR-02102-3] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Teil 3 - Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2). Technical Guideline. Version 2019-02. Bundesamt für Sicherheit in der Informationstechnik (BSI), 11. Feb. 2019. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.

[TR-03111] Bundesamt für Sicherheit in der Informationstechnik. *Elliptic Curve Cryptography*. Technische Richtlinie BSI TR-03111. Technical Guideline. Version 2.10. Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. Juni 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.

[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-03157] Bundesamt für Sicherheit in der Informationstechnik. *Konnektor – Prüfspezifikation für das Fachmodul ePA*. Technische Richtlinie BSI TR-03157. Technical Guideline. Version 2.0. Bundesamt für Sicherheit in der Informationstechnik (BSI), 3. Aug. 2021.

Herstellerdokumente

[AGD_ADM-Erg] KoCo Connector GmbH. *Ergänzungen zum Administratorhandbuch KoCoBox MED+ Version 5*. Version 1.3.4. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2024.

[AGD_ADM] KoCo Connector GmbH. *Administratorhandbuch KoCoBox MED+ Version 5*. Version 5. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 17. Juli 2024.

[AGD_JSON] KoCo Connector GmbH. *JSON-Managementschnittstelle der KoCoBox MED+. Dokumentation*. Version 3.22. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2024.

[AGD_Kon-Sec] KoCo Connector GmbH. *KoCoBox MED+ Konnektor. Konnektor Security Guidance Fachmodule NFDM, AMTS und ePA*. Programmierrichtlinien für die Entwickler von Fachmodulen. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2024.

[ALC_DEL] KoCo Connector GmbH. *KoCoBox MED+ Konnektor. Delivery Procedures (ALC_DEL)*. Common Criteria Komponente ALC_DEL. Version 1.3.6. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2023.

[ASE_ST-97] KoCo Connector GmbH. *KoCoBox MED+ Netzkonnektor. Security Target*. Common Criteria Komponente ASE_ST. Vorgelegt im Verfahren BSI-DSC-CC-1067-V5 zu BSI-CC-PP-0097. 2024.

[ASE_ST-98] KoCo Connector GmbH. *KoCoBox MED+ Konnektor. Security Target*. Common Criteria Komponente ASE_ST. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2024.

[FM-API] KoCo Connector GmbH. *KoCoBox MED+ Konnektor. Konnektor API für Fachmodule Javadoc*. Common Criteria Komponente AGD. Vorgelegt im Verfahren BSI-DSC-CC-1068-V5 zu BSI-CC-PP-0098. 2024.

gematik Spezifikationen

[gemF_LZV_gSMC-K] gematik GmbH. *Feature Laufzeitverlängerung gSMC-K*. Version 1.2.0. Referenzierung der gematik als „gemF_Laufzeitverlängerung_gSMC-K“. 17. Apr. 2023.

[gemILF_PS] gematik GmbH. *Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI)*. einschließlich VSDM, QES-Basisdienste, KOM-LE. Version 2.17.0. Revision 522766. 28. Nov. 2022.

[gemKPT_Arch_TIP] gematik GmbH. *Konzept. Architektur der TI-Plattform*. Version 2.10.0. Revision 198478. 2. März 2020.

[gemProdT_Kon_PTV5P] gematik GmbH. *Produkttypsteckbrief Konnektor*. Prüfvorschrift. Produkttyp Version PTV5Plus 5.54.1-0. Version 1.0.0. Referenzierung der gematik als „gemProdT_Kon_PTV5Plus_5.54.1-0“. 9. März 2023.

[gemSpec_Kon] gematik GmbH. *Spezifikation Konnektor*. Version 5.18.0. Revision 531891. 28. Nov. 2022.

[gemSpec_Krypt] gematik GmbH. *Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur*. Version 2.26.0. Revision 58881. 9. März 2023.

[gemSpec_Net] gematik GmbH. *Übergreifende Spezifikation Netzwerk*. Version 1.23.0. Revision 539758. 16. Dez. 2022.

[gemSpec_OID] gematik GmbH. *Spezifikation Festlegung von OIDs*. Version 3.11.0. Revision 432563. 21. Jan. 2022.

[gemSpec_PKI] gematik GmbH. *Übergreifende Spezifikation PKI*. Version 2.14.1. Revision 541391. 16. Dez. 2022.

[gemWSDL-TI] gematik GmbH. *Schnittstellendefinitionen TI im XSD- und WSDL-Format*. Datum entspricht dem Datum des Tags im Repository. 21. Juni 2022. URL: https://github.com/gematik/api-telematik/releases/tag/4.1.2.

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 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 186-4] 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 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.

[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*. NIST Special Publication 800-90A. Version Revision 1. National Institute of Standards und Technology, Juni 2015. URL: http://doi.org/10.6028/NIST.SP.800-90Ar1.

RFC

[RFC 2104] H. Krawczyk, M. Bellare und R. Canetti. *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104 (Informational). RFC. Updated by RFC 6151. Fremont, CA, USA: RFC Editor, Feb. 1997. DOI: 10.17487/RFC2104. URL: https://www.rfc-editor.org/rfc/rfc2104.txt.

[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 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 3602] S. Frankel, R. Glenn und S. Kelly. *The AES-CBC Cipher Algorithm and Its Use with IPsec*. RFC 3602 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Sep. 2003. DOI: 10.17487/RFC3602. URL: https://www.rfc-editor.org/rfc/rfc3602.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 4106] J. Viega und D. McGrew. *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*. RFC 4106 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Juni 2005. DOI: 10.17487/RFC4106. URL: https://www.rfc-editor.org/rfc/rfc4106.txt.

[RFC 4301] S. Kent und K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301 (Proposed Standard). RFC. Updated by RFCs 6040, 7619. Fremont, CA, USA: RFC Editor, Dez. 2005. DOI: 10.17487/RFC4301. URL: https://www.rfc-editor.org/rfc/rfc4301.txt.

[RFC 4303] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Dez. 2005. DOI: 10.17487/RFC4303. URL: https://www.rfc-editor.org/rfc/rfc4303.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 5282] D. Black und D. McGrew. *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*. RFC 5282 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2008. DOI: 10.17487/RFC5282. URL: https://www.rfc-editor.org/rfc/rfc5282.txt.

[RFC 5289] E. Rescorla. *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*. RFC 5289 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2008. DOI: 10.17487/RFC5289. URL: https://www.rfc-editor.org/rfc/rfc5289.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 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 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“. Technische Anlage. In: *Deutsches Ärzteblatt* (Okt. 2018). URL: http://daebl.de/MA27.

[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.

[STARCOS-ST_36] Giesecke+Devrient Mobile Security GmbH. *Security Target Lite. STARCOS 3.6 COS C1*. Version 1.5. 31. Juli 2017.

[STARCOS-ST_37] Giesecke+Devrient Mobile Security GmbH. *Security Target Lite. STARCOS 3.7 COS HBA-SMC*. Version 1.0. 18. Mai 2021.

[TCOS-ST] Ernst-G. Giessmann und Markus Blick. *Specification of the Security Target TCOS FlexCert*. Version 2.0 Release 2/SLC52. Version 2.0.2. Deutsche Telekom Security GmbH. 25. Mai 2021.

Verzeichnis der ST-Anwendungshinweise

Index der SFR