Common Criteria Certification
BSI-DSZ-CC-1068-V5 BSI-CC-PP-0098

Security Target
Konnektor

KoCoBox MED+ Konnektor
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 TR Zertifizierung

Die KoCoBox MED+ dient als Ablaufplattform für die Fachmodule NFDM, AMTS und ePA. Diese Fachmodule sind nicht Teil der Common Criteria Zertifizierung des Gesamtkonnektors. Stattdessen werden sie nach Technischen Richtlinien zertifiziert, vgl. Tabelle 1. Die TR stellen Anforderungen an die CC-Zertifizierung des Konnektors: Der Konnektor muss bestimmte Eigenschaften aufweisen. Es ist Aufgabe des CC-Zertifzierers, die Erfüllung dieser Anforderungen zu bestätigen.

Obwohl keine formale Übereinstimmung mit den TR behauptet wird, spielen die TR eine wichtige Rolle für die CC-Zertifzierung. Das drückt sich in diesem Security Target dadurch aus, dass die

Konformitätserklärung in Kapitel 2 um einen Abschnitt erweitert wurde. Weiterhin wird in Kapitel 8 beschrieben, wie die KoCoBox MED+ die Anforderungen erfüllt.

Fachmodul	gematik Spezifikation		Technische Richtlinie	
NFDM	[gemSpec_FM_NFDM]	v1.6.2, 30. Juni 2021	[TR-03154]	v1.1, 15. Apr. 2019
AMTS	[gemSpec_FM_AMTS]	v1.4.0, 15. Mai 2019	[TR-03155]	v1.1, 15. Apr. 2019
ePA	[gemSpec_FM_ePA]	v1.52.0, 1. Dez. 2022	[TR-03157]	v2.0, 3. Aug. 2021

Tabelle 1.: Spezifikationen und TR der Fachmodule der KoCoBox MED+

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]. Abschnitt 2.6 präzisiert den Zusammenhang zwischen dem Security Target und der Spezifikation der gematik.

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

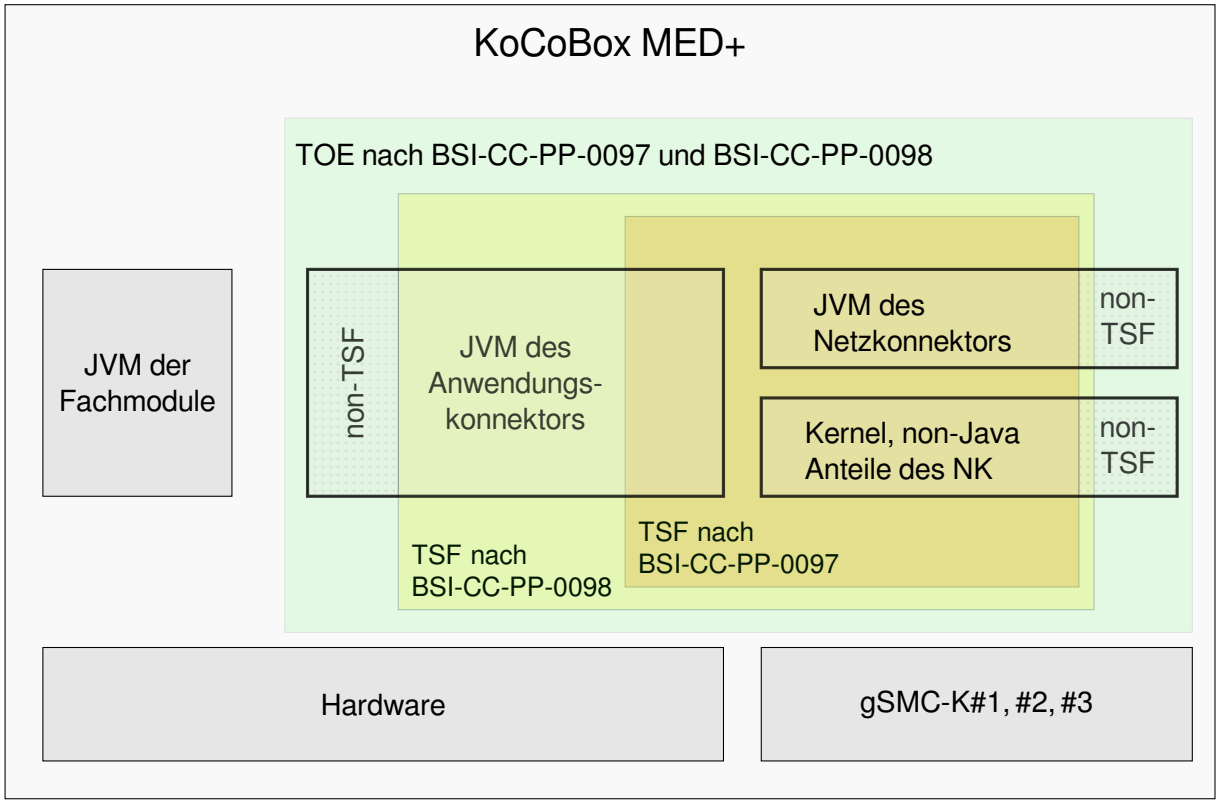


Abbildung 1.: Abgrenzung der Verfahren zu BSI-CC-PP-0097 und BSI-CC-PP-0098

Inhaltsverzeichnis

1. Einführung in das Security Target **12**
- 1.1. ST Referenz . . . 12
- 1.2. TOE Referenz . . . 12
- 1.3. Überblick über den TOE . . . 13
  - 1.3.1. TOE Typ . . . 13
  - 1.3.2. Verwendung und Hauptfunktionalität des TOE . . . 13
  - 1.3.3. Erforderliche Non-TOE Hardware/Software/Firmware . . . 13
- 1.4. Beschreibung des TOE . . . 14
  - 1.4.1. Hauptziele des TOE . . . 14
  - 1.4.2. Aufbau des TOE . . . 15
  - 1.4.3. Einsatzumgebung des TOE . . . 15
  - 1.4.4. Hardware der KoCoBox MED+ . . . 17
  - 1.4.5. Schnittstellen des Konnektors . . . 23
  - 1.4.6. Aufbau und physische Abgrenzung des Konnektors PTV 5+ . . . 28
  - 1.4.7. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste . . . 29
  - 1.4.8. Physischer Umfang des TOE . . . 31

2. Postulat der Übereinstimmung **33**
- 2.1. Konformität zu Common Criteria . . . 33
- 2.2. Konformität zu Schutzprofilen . . . 33
- 2.3. Konformität zu Paketen . . . 33
- 2.4. Erklärung der Konformität . . . 33
- 2.5. Konformität zu Technischen Richtlinien für Fachmodule . . . 34
- 2.6. Konformität zur Prüfvorschrift „Konnektor“ . . . 34

3. Definition des Sicherheitsproblems **35**
- 3.1. Werte . . . 35
  - 3.1.1. Zu Schützende Werte . . . 35
  - 3.1.2. Benutzer des TOE . . . 35
- 3.2. Bedrohungen . . . 35
- 3.3. Organisatorische Sicherheitspolitiken . . . 36
- 3.4. Annahmen . . . 37

4. Sicherheitsziele **38**
- 4.1. Sicherheitsziele für den Netzkonnektor . . . 38
  - 4.1.1. Allgemeine Ziele: Schutz und Administration . . . 38
  - 4.1.2. Ziele für die VPN Funktionalität . . . 39
  - 4.1.3. Ziele für die Paketfilter-Funktionalität . . . 39

4.2. Sicherheitsziele für den Anwendungskonnektor . . . 39
4.2.1. Allgemeine Sicherheitsziele . . . 39
4.2.2. Signaturdienst . . . 40
4.2.3. Gesicherte Kommunikation / TLS Proxy . . . 41
4.2.4. Terminal- und Chipkartendienst . . . 41
4.2.5. Verschlüsselungsdienste . . . 42
4.2.6. Fachmodul VSDM . . . 42
4.3. Sicherheitsziele für die Umgebung des Netzkonnektors . . . 42
4.4. Sicherheitsziele für die Umgebung des Anwendungskonnektors . . . 44
4.5. Erklärung der Sicherheitsziele des Netzkonnektors . . . 46
4.5.1. Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele . . . 46
4.6. Erklärung der Sicherheitsziele des Anwendungskonnektors . . . 48

5. Definition der erweiterten Komponenten 49
5.1. Definition der erweiterten Familie FCS_RNG . . . 49
5.2. Definition der erweiterten Familie FPT_EMS . . . 50
5.3. Definition der erweiterten Familie FIA_API . . . 50

6. Sicherheitsanforderungen 51
6.1. Hinweise und Definitionen . . . 51
6.1.1. Hinweise zur Notation . . . 51
6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen . . . 51
6.2. Funktionale Sicherheitsanforderungen des Netzkonnektors . . . 53
6.2.1. VPN Client . . . 53
6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung . . . 54
6.2.3. Netzdienste . . . 60
6.2.4. Stateful Packet Inspection . . . 62
6.2.5. Selbstschutz . . . 62
6.2.6. Administration . . . 64
6.2.7. Kryptographische Basisdienste . . . 67
6.2.8. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen . . . 70
6.2.9. Zusätzliche Sicherheitsanforderungen . . . 77
6.3. Funktionale Sicherheitsanforderungen des Anwendungskonnektors . . . 80
6.3.1. Klasse FCS: Kryptographische Unterstützung . . . 80
6.3.2. Klasse FIA: Identifikation und Autorisierung . . . 87
6.3.3. Klasse FDP: Schutz der Benutzerdaten . . . 92
6.3.4. Klasse FMT: Sicherheitsmanagement . . . 142
6.3.5. Klasse FPT: Schutz der TSF . . . 147
6.3.6. Klasse FAU: Sicherheitsprotokollierung . . . 151
6.3.7. VAU Protokoll . . . 153
6.3.8. SGD Protokoll / ECIES Verfahren . . . 158
6.4. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG . . . 165
6.4.1. Verfeinerung zur Vertrauenswürdigkeitskomponente ADV_ARC.1 . . . 165
6.4.2. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_OPE.1 . . . 165
6.4.3. Verfeinerung zur Vertrauenswürdigkeitskomponente ALC_DEL.1 . . . 165
6.4.4. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_PRE.1 . . . 165

6.4.5. Verfeinerung für die Integration der Fachmodule NFDM, AMTS und ePA . 165
6.5. Erklärung der Sicherheitsanforderungen 166
6.5.1. Erklärung der Abhängigkeiten der SFR des Netzkonnektors 166
6.5.2. Überblick der Abdeckung von Sicherheitszielen des Netzkonnektors 167
6.5.3. Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors 167
6.5.4. Erklärung der Abhängigkeiten der SFR des Anwendungskonnektors 168
6.5.5. Überblick der Abdeckung von Sicherheitszielen des Anwendungskonnektors 169
6.5.6. Detaillierte Erklärung für die Sicherheitsziele des Anwendungskonnektors . . 171
6.6. Erklärung für Erweiterung der Sicherheitsanforderungen 172
6.7. Erklärung für die gewählte EAL-Stufe 173

7. ASE_TSS: Basiskonnektor 174
7.1. TOE Sicherheitsfunktionen des Netzkonnektors 174
7.1.1. VPN-Client (SF.VPN) 174
7.1.2. Dynamischer Paketfilter (SF.DynamicPacketFilter) 175
7.1.3. Netzbasierte Sicherheitsfunktionen (SF.NetworkServices) 177
7.1.4. Selbstschutz (SF.SelfProtection/NK) 177
7.1.5. Protokollierungsdienst/NK (SF.Audit/NK) 179
7.1.6. Administration/NK (SF.Administration/NK) 179
7.1.7. Kryptografische Dienste/NK (SF.CryptographicServices/NK) 181
7.2. TOE Sicherheitsfunktionen des Konnektors 185
7.2.1. Kryptografische Dienste/AK (SF.CryptographicServices/AK) 185
7.2.2. TLS Protokoll (SF.TLS) 186
7.2.3. Authentisierung (SF.Authentication) 186
7.2.4. Zugriffssteuerung (SF.AccessControl) 188
7.2.5. Management der eHealth-Kartenterminals (SF.CardTerminalMgmt) 189
7.2.6. Management der Smart Cards (SF.SmartCardMgmt) 190
7.2.7. Signaturdienst (SF.SignatureService) 191
7.2.8. Verschlüsselungsdienst (SF.EncryptionService) 197
7.2.9. Sicherer Speicher (SF.SecureStorage) 199
7.2.10. Versichertenstammdatenmanagement (SF.VSDM) 199
7.2.11. Administration/AK (SF.Administration/AK) 200
7.2.12. Selbstschutz (SF.SelfProtection/AK) 201
7.2.13. Protokollierungsdienst/AK (SF.Audit/AK) 203
7.3. TOE Sicherheitsfunktionen für Fachmodule 204
7.3.1. VAU-Protokoll (SF.VAU) 204
7.3.2. SGD-Protokoll / ECIES-Verfahren (SF.SGD) 207
7.4. Verhältnis von SFR zu SF des Netzkonnektors 211
7.5. Verhältnis von SFR zu SF des Konnektors 213

8. ASE_TSS: Fachmodule 217
8.1. Erklärung der Konformität zu Technischen Richtlinien 217
8.1.1. Fachmodule NFDM und AMTS / PTV 3 217
8.1.2. Fachmodul ePA / PTV 4 218
8.2. Umsetzung der TUCs an LS.FM im Basiskonnektor 219

A. Erklärung der tabellarischen Darstellung **227**

B. TLS Verbindungen **228**

C. Composition Requirements für Fachmodule **232**

D. Anforderungen zur sicherheitstechnischen Eignung **234**

Literatur **246**

Index der gematik Anforderungen **259**

Index der SFR **261**

Tabellenverzeichnis

1. Spezifikationen und TR der Fachmodule der KoCoBox MED+ 3

1.2. Logische Schnittstellen an LS.LAN 25
1.3. Logische Schnittstellen an LS.WAN 26
1.4. Logische Schnittstellen an LS.VPN_TI 26
1.5. Logische Schnittstellen an LS.VPN_SIS 26
1.6. Logische Schnittstellen an LS.FM 27
1.7. Physischer Umfang des TOE 32

2.1. Ergänzungen zur Vertrauenswürdigkeit EAL3 33

3.1. Primäre Werte des Anwendungskonnektors 36

4.1. Abbildung der Sicherheitsziele des Netzkonnektors auf Bedrohungen und Annahmen 47

6.1. Typographische Konventionen 52
6.2. Objekte des TOE 52
6.3. Algorithms, Key sizes/Curve and Purposes of Signature Verification for NK 79
6.4. Algorithms, Key sizes/Curve of Signature Verification of BNetzA-VL 85
6.6. Abbildung der Sicherheitsziele des NK auf *eigene* Sicherheitsanforderungen 167
6.5. Abhängigkeiten der hinzugefügten SFR des Netzkonnektors 167
6.7. Abhängigkeiten der hinzugefügten SFR 169
6.8. Abbildung der Sicherheitsziele des AK auf *eigene* Sicherheitsanforderungen 170

7.1. Algorithmen für nonQES 183
7.2. Algorithmen für nonQES 183
7.3. Signaturvarianten 195
7.4. TLS Parameter für die Verbindung zur Management-Webanwendung 202
7.5. TLS Parameter für die Verbindung zum KSR-Service 202
7.6. Abbildung der SFR des NK auf Sicherheitsfunktionalitäten 212
7.7. Abbildung der SFR des AK auf Sicherheitsfunktionalitäten 216

8.1. SFR-Zuordnung der TUCs für Fachmodule 222
8.2. Funktionen des Basiskonnektors für die Fachmodule 226

A.1. Legende der Abbildungstabellen 227

B.1. Cipher Suites der TLS Verbindungen des Konnektors 228
B.2. Elliptische Kurven für die TLS Verbindungen des Konnektors 228
B.3. Signaturalgorithmen für die TLS Verbindungen des Konnektors 228
B.4. Legende zu den TLS Verbindungen 229

B.5. TLS Verbindungen der KoCoBox MED+ 230
B.6. Identität des TOE bei TLS-Verbindungen 231

D.1. Erweiterung des Security Targets für PTV 5+ 245

Abbildungsverzeichnis

1. Abgrenzung der Verfahren zu BSI-CC-PP-0097 und BSI-CC-PP-0098 4

1.1. Einsatzumgebung der KoCoBox MED+ 15
1.2. Gehäuse der Generation 3 (G3) 18
1.3. Hardware-Komponenten der Generation 3 (G3) 19
1.4. Gehäuse der KoCoBox MED+ (G4) 21
1.5. Hardware-Komponenten der KoCoBox MED+ (G4) 22

1. Einführung in das Security Target

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

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

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

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

1.1. ST Referenz

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

1.2. TOE Referenz

Evaluierungsgegenstand	KoCoBox MED+ Konnektor
Version des EVG	5.5.12
Hersteller	KoCo Connector GmbH
Vertrauenswürdigkeitsstufe	EAL3 erweitert um AVA_VAN.3, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 (Kurzbezeichnung „EAL3+“)
CC Version	3.1 Release 5

1.3. Überblick über den TOE

Der Evaluierungsgegenstand ist der Konnektor in der Produkttypversion PTV 5+. Der TOE umfasst folgende Komponenten:

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

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

1.3.1. TOE Typ

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

1.3.2. Verwendung und Hauptfunktionalität des TOE

Der TOE ist eine sichere Komponente, die in der Telematikinfrastrukur als Konnektor eingesetzt wird. Die Funktionalität der KoCoBox MED+ geht aus der Konnektor-Spezifikation der gematik [gemSpec_Kon] hervor. Darüber hinaus finden weitere Spezifikationen der gematik Beachtung (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

[1] Im folgenden wird der Einfachheit halber angenommen, dass die Einsatzumgebung eine Arztpraxis ist.

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+.

1.4. Beschreibung des TOE

1.4.1. Hauptziele des TOE

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

Sichere Verbindung in die Telematikinfrastruktur

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

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

Kontrolle von Kartenterminals und Smart Cards

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

Signaturkomponente und Dokumentenverschlüsselung

Zusätzlich zu diesen Hauptzielen stellt der Konnektor noch eine 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.

[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-0098].

[3] oder eine andere Zugangstechnologie

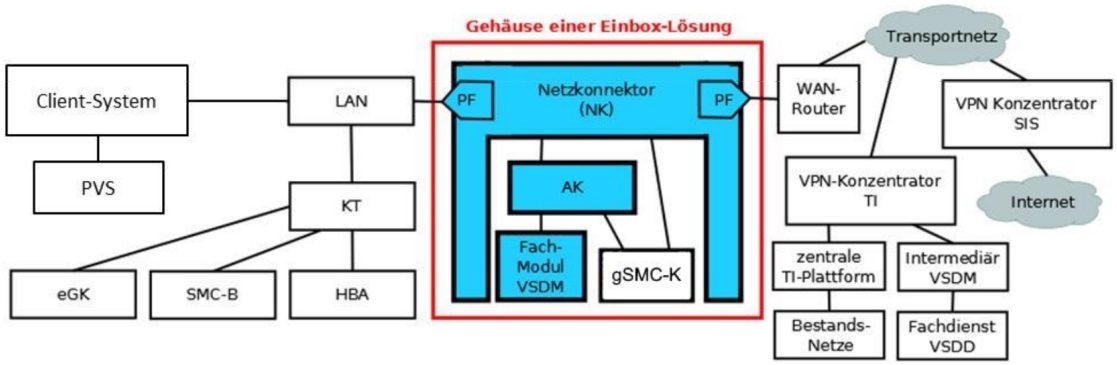


Abbildung 1.1.: Einsatzumgebung der KoCoBox MED+

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 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. 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.

[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.

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.

Abbildung 1.2.: Gehäuse der Generation 3 (G3)

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 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.

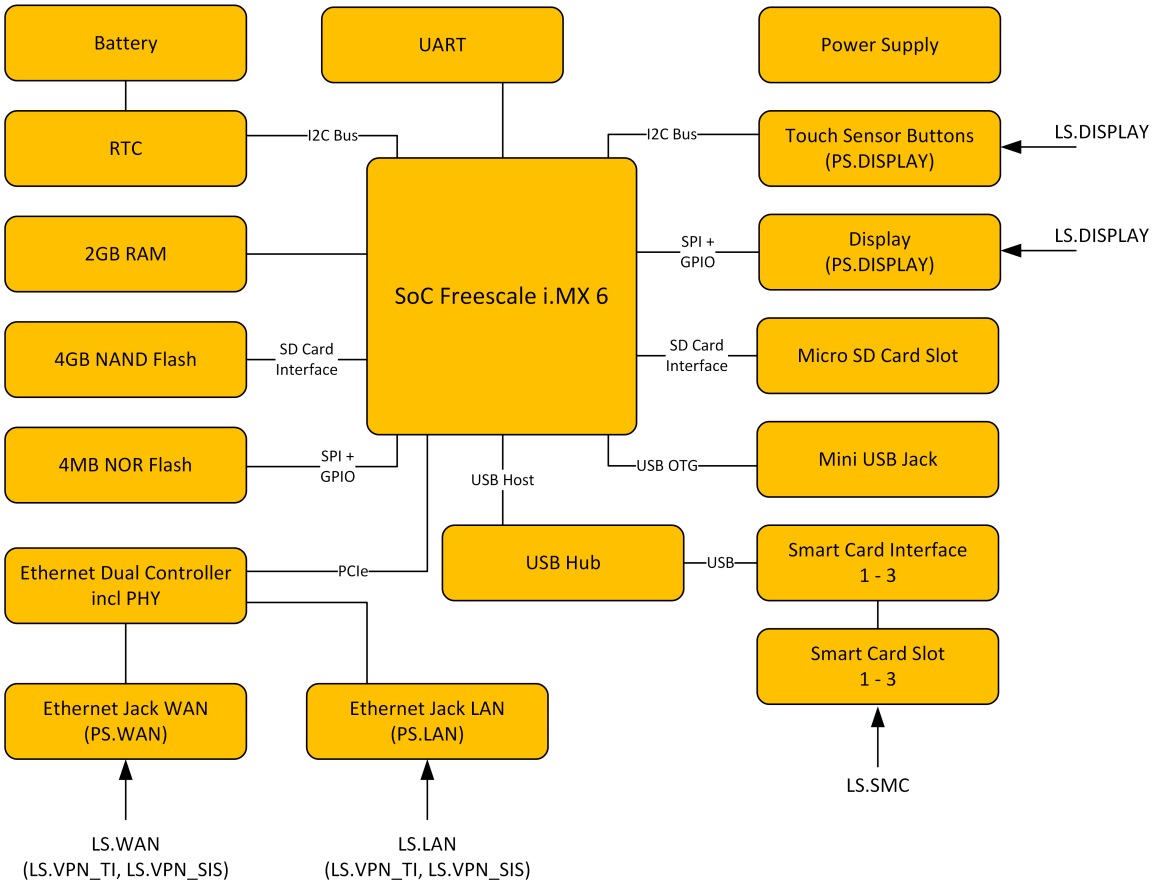


Abbildung 1.3.: Hardware-Komponenten der Generation 3 (G3). Die logischen Schnittstellen des TOE sind in dem Diagramm als von außen an die Systemkomponenten heranreichende Pfeile repräsentiert. Die entsprechenden physischen Schnittstellen sind in den äußeren Komponenten eingetragen.

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 19 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 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 22 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.

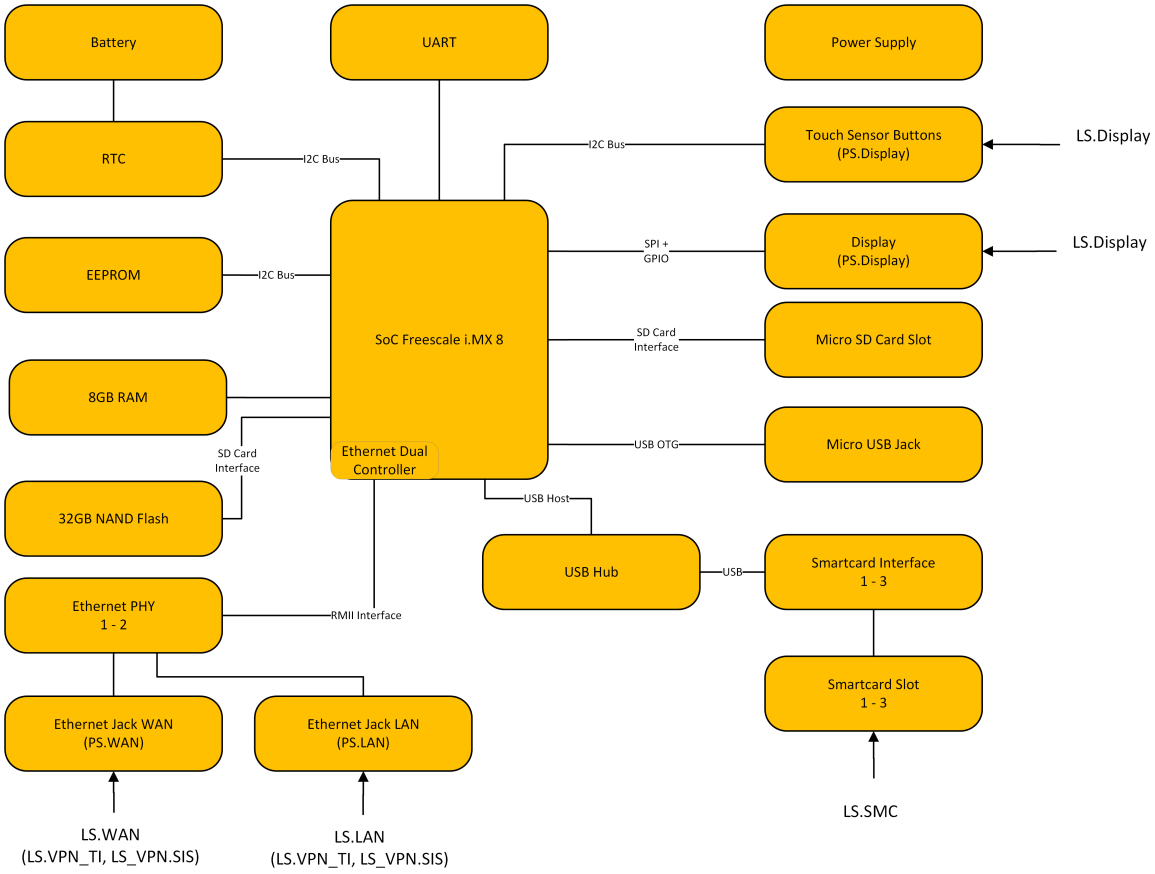


Abbildung 1.5.: Hardware-Komponenten der Generation 4 (G4). Die logischen Schnittstellen des TOE sind in dem Diagramm als von außen an die Systemkomponenten heranreichende Pfeile repräsentiert. Die entsprechenden physischen Schnittstellen sind in den äußeren Komponenten eingetragen.

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.

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

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

Bezeichner	Rolle	Zweck der Schnittstelle
LS.LAN.CETP	Client	Übertragung von Systemereignissen an Clientsysteme
LS.LAN.DHCP	Server	Adressvergabe im LAN
LS.LAN.DNS	Server	Auflösung von Hostnamen im LAN
LS.LAN.Ether	—	Protokoll auf Zugangsschicht
LS.LAN.HTTP	Server	HTTP Zugriff auf Basisdienste
LS.LAN.HTTP_Client	Client	CRL Download
LS.LAN.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.

1.4.7.2. Sicherheitsdienste des Anwendungskonnektors

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

Gesicherte Kommunikation Die „Fachdienste“ aus dem zweiten Spiegelstrich werden hier erweitert um die Verbindung zu den Fachdiensten der elektronischen Patientenakte. Der Konnektor implementiert – konform zur Technischen Richtlinie des Fachmodul ePA [TR-03157] – die Protokolle zur Kommmunikation mit dem Schlüsselgenerierungsdienst (SGD) und der vertrauenswürdigen Ausführungsumgebung (VAU).

Versichertenstammdatenmanagment (VSDM) Der Anwendungskonnektor implementiert das Fachmodul VSDM als Teil des Basiskonnektors.

Darüber hinaus implementiert auch der Anwendungskonnektor – genau wie der Netzkonnektor – Mechanismen zum Selbstschutz, zur Durchführung von Selbsttests, zur Protokollierung und zur Administration des Konnektors.

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

Dieses Security Target behauptet keine Konformität zu weiteren Schutzprofilen.

2.3. Konformität zu Paketen

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

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

Tabelle 2.1.: Ergänzungen zur Vertrauenswürdigkeit EAL3

2.4. Erklärung der Konformität

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

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

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

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

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

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

2.5. Konformität zu Technischen Richtlinien für Fachmodule

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

- „*Konnektor – Prüfspezifikation für das Fachmodul NFDM*“ [TR-03154, Abschnitt 3.3.2]
- „*Konnektor – Prüfspezifikation für das Fachmodul AMTS*“ [TR-03155, Abschnitt 3.3.2]
- „*Konnektor – Prüfspezifikation für das Fachmodul ePA*“ [TR-03157, Abschnitt 3.2.2]

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

2.6. Konformität zur Prüfvorschrift „Konnektor“

Dieses Security Target erfüllt weiterhin die Forderung der gematik aus Abschnitt 3.2.1 (CC-Evaluierung) der Prüfvorschrift für den Produkttyp „Konnektor“ in Version PTV 5+ [gemProdT_Kon_PTV5P]. Der Produkttypsteckbrief fordert, dass der Hersteller die Abdeckung der Anforderungen, die nicht durch das Schutzprofil erklärt sind, im Security Target dokumentiert. Dies erfolgt hier durch die explizite Nennung der Anforderungen in der *TOE Summary Specification* (ASE_TSS) in Kapitel 7 und durch die Auflistung in Anhang D. Diese Auflistung ist als *Teil von ASE_TSS* zu verstehen und in die Prüfung einzubeziehen.[1]

[1] Weiterhin gibt es bei der Beschreibung der SFR eine weitere Auszeichnungsfarbe für Operationen, die durch die Prüfvorschrift „Konnektor“ motiviert sind (Vgl. die Erläuterungen in Unterabschnitt 6.1.1).

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“ sowohl für den NK als auch für den AK subsumiert. Für sie gelten die Schutzziele Integrität und – bei der Übertragung – Authentizität [gemF_LZV_gSMC-K].

Im Zuge der Hinzunahme der Fachanwendung ePA wird die Liste der durch den Anwendungskonnektor zu schützenden Werte um die Angaben in Tabelle 3.1 auf der nächsten Seite erweitert.

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.

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, davon abgeleitete Bedrohungen und Annahmen
VAU/SGD-Inhaltsdaten	Integrität, Authentizität, Vertraulichkeit	Nutzerdaten und Metadaten, die vom EVG zur Verarbeitung an den VAU-Server-Endpunkt des ePA-Aktensystems (betrifft ePA-Schlüsselmaterial und ePA-Metadaten) bzw. in das SGD-HSM (betrifft SGD-AES-Schlüssel) übergeben werden, bzw. von diesen empfangen werden, dürfen bei der Übermittlung weder unbemerkt verändert noch unbefugt eingesehen werden. Zudem dürfen sie nur an authentisierte Kommunikationspartner geschickt werden. ⇒ OSP.AK.VAUSGD

Tabelle 3.1.: Primäre Werte des Anwendungskonnektors

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.

OSP.AK.VAUSGD

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

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 den Anwendungskonnektor

4.2.1. Allgemeine Sicherheitsziele

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

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

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

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

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

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

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

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

4.2.2. Signaturdienst

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

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

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

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

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

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

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

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

O.AK.Sig.Komfortsignatur (Komfortsignatur)
Der EVG bietet die Komfortsignatur nach PTV4+ gemäß *Spezifikation Konnektor* [gemSpec_Kon]. Das Sicherheitsziel stellt sicher, dass Komfortsignaturen ausschließlich dann erstellt werden, wenn die bereitgestellten Sessions des HBA den korrekten Authentisierungsstatus haben. Jeder HBA stellt drei voneinander unabhängig nutzbare Cardsessions bereit.

4.2.3. Gesicherte Kommunikation / TLS Proxy

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

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

O.AK.VAUSGD (gesicherte Kommunikation zwischen EVG und VAU sowie zwischen EVG und SGD-HSM)
Der EVG bietet eine gesicherte Kommunikationsverbindung mittels „VAU-Protokoll“ zum VAU-Server-Endpunkt des ePA-Aktensystems und mittels „SGD-Protokoll“ in das SGD-HSM des Schlüsselgenerierungsdienst an, sodass das Abhören von Daten für diese Kommunikation unterbunden ist. Das VAU-Protokoll ist gemäß der Spezifikation umgesetzt [gemSpec_Krypt, Kapitel 6]. Das SGD-Protokoll ist gemäß den Vorgaben in den Spezifikationen umgesetzt. Der Protokollablauf wird in der Spezifikation des Schlüsselgenerierungsdienst definiert [gemSpec_SGD_ePA, Kapitel 2.3], die kryptographischen Eigenschaften in der *Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur* [gemSpec_Krypt, Abschnitt 3.15.5].

4.2.4. Terminal- und Chipkartendienst

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

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

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

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

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

4.2.5. Verschlüsselungsdienste

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

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

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

4.2.6. Fachmodul VSDM

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

4.3. Sicherheitsziele für die Umgebung des Netzkonnektors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.4. Sicherheitsziele für die Umgebung des Anwendungskonnektors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OE.AK.Karten (Chipkarten im LAN des Leistungserbringers)
Das in Abschnitt 4.4 von [BSI-CC-PP-0098] beschriebene Sicherheitsziel OE.AK.Karten muss erfüllt werden.

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

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

Wenn das Clientsystem die Funktion Komfortsignatur des Konnektors verwendet, muss das Clientsystem eine hinreichend sichere User ID generieren, die es dem Konnektor beim Aktivieren der Komfortsignatur übergibt. Für die Verwendung der Komfortsignaturfunktionalität muss das zum Einsatz kommende Clientsystem pro Aktivierung der Komfortsignaturfunktion eine eindeutige UserID im Format UUID gemäß RFC 4122 [RFC 4122] generieren. Hierzu muss durch das Clientsystem mithilfe eines qualitativ guten Zufallszahlengenerators [AIS 20; AIS 31; NIST SP 800-90A] benötigter Zufall in einer Menge von 128 bit erzeugt, bereitgestellt und verwendet werden. Dieser Zufall muss damit praktisch unvorhersagbar sein (oder nur erratbar mit einer Wahrscheinlichkeit von 2^{-128}). Jede UserID zur Verwendung der Komfortsignatur-

funktionalität muss im Clientsystem eindeutig einem Benutzer (User) zugeordnet sein. Sie ist weiterhin durch das Clientsystem sowie den zugeordneten Benutzer vertraulich zu behandeln. Auf die Notwendigkeit der vertraulichen Behandlung der UserID ist in der Dokumentation des Clientsystems hinzuweisen.

Weiterhin muss das Clientsystem den Benutzer beim Verwenden der Komfortsignatur authentifizieren. Die Authentifizierung des Nutzers am Clientsystem leistet einen unverzichtbaren Beitrag zur Sicherheit des Konnektors (vgl. A_19101).

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

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

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

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

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

4.5. Erklärung der Sicherheitsziele des Netzkonnektors

4.5.1. Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele

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

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

4.5.1.1. Abwehr der Bedrohungen durch die Sicherheitsziele

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

	O.NK.TLS_Krypto	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.gSMC-K	OE.NK.KeyStorage	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.Admin_Auth	OE.NK.PKI	OE.NK.phys_Schutz	OE.NK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betrieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS
T.NK.Local_EVG_LAN	.	✓	.	.	✓	✓	.	.	.	.	.	✓	–	.	✓	✓	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
T.NK.remote_EVG_WAN	.	✓	.	.	✓	✓	✓	✓	.	✓	✓	.	✓	✓	✓	✓	✓	✓	.	.	.	.	✓	.	✓	.	.	.	✓	.
T.NK.remote_EVG_LAN	.	✓	.	.	✓	✓	✓	✓	.	✓	✓	✓	✓	✓	✓	✓	✓	✓	.	.	.	.	✓	.	✓	.	.	✓	✓	✓
T.NK.remote_VPN_Data	.	.	.	–	✓	✓	✓	✓	✓	.	.	.	✓	✓	✓	✓	✓	✓	✓	.	.	.	✓	.	✓	.	✓	✓	✓	✓
T.NK.local_admin_LAN	.	✓	.	✓	✓	✓	.	.	.	.	.	–	–	✓	✓	✓	.	✓	.	.	✓	✓	–	–	.	.	.	.	–	.
T.NK.remote_admin_WAN	.	✓	.	✓	✓	✓	.	.	.	.	–	.	–	✓	✓	✓	.	✓	.	.	✓	✓	–	.	.	.	.	.	–	.
T.NK.counterfeit	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	✓	.	.	.	.	✓	.
T.NK.Zert_Prüf	.	.	.	.	–	–	.	✓	.	.	–	.	–	–	–	–	–	.	.	.	.	.	✓	.	.	.	.	.	✓	.
T.NK.TimeSync	.	.	.	.	–	✓	✓	✓	.	✓	–	.	–	✓	✓	✓	✓	.	.	.	.	.	✓	.	.	.	.	.	✓	.
T.NK.DNS	.	.	.	.	–	–	✓	✓	.	.	–	.	–	.	–	–	.	.	.	.	.	.	✓	.	.	.	.	✓	✓	–
OSP.NK.Zeitdienst	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	✓	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
OSP.NK.SIS	.	.	.	.	.	.	.	.	.	.	✓	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
OSP.NK.BOF	.	.	.	.	.	.	✓	✓	✓	✓	✓	.	✓	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
OSP.NK.TLS	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
A.NK.phys_Schutz	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.
A.NK.gSMC-K	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
A.NK.sichere_TI	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
A.NK.kein_Dos	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
A.NK.AK	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.
A.NK.CS	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
A.NK.Betrieb_AK	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
A.NK.Betrieb_CS	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
A.NK.Admin_EVG	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
A.NK.Ersatzverfahren	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
A.NK.Zugriff_gSMC-K	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	✓	.	.	.

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

4.5.1.2. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

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

4.5.1.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

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

4.6. Erklärung der Sicherheitsziele des Anwendungskonnektors

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

OSP.AK.VAUSGD
Die zusätzlich aufgenommene Sicherheitspolitik OSP.AK.VAUSGD wird wie folgt auf die Sicherheitsziele abgebildet:

- O.AK.VAUSGD fordert die Konformität des TOE zu den Spezifikationen des VAU-Protokolls und des SGD-Protokolls, sodass die Kommunikation mit dem VAU-Server-Endpunkt und dem SGD-HSM nicht abgehört werden können.
- OE.AK.Fachdienste sieht vor, dass die Fachdienste der TI – also auch der VAU-Server-Endpunkt und das SGD-HSM – als vertrauenswürdig anzusehen sind und keine Angriffe über bestehende Kommunikationskanäle auf den AK erfolgen. Dieses Ziel der Umgebung ist konform mit der OSP, dass VAU/SGD-Inhaltsdaten gegen einen passiven Angreifer geschützt werden müssen, der die Daten mithört, aber nicht manipuliert.

O.AK.Sig.Komfortsignatur
Das zusätzlich angenommene Sicherheitsziel O.AK.Sig.Komfortsignatur beschreibt eine Variante der Stapelsignatur. Folglich gelten alle Abbildungen des Sicherheitsziels O.AK.Sig.Stapelsignatur auch für das Ziel O.AK.Sig.Komfortsignatur. Es gibt keine zusätzliche Relation zu anderen/neuen Sicherheitsproblemen, die über die Relationen von O.AK.Sig.Stapelsignatur hinausgehen.

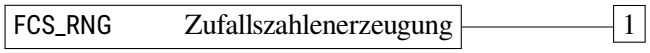
5. Definition der erweiterten Komponenten

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] und [BSI-CC-PP-0098] übernommen.

5.3. Definition der erweiterten Familie FIA_API

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

6. Sicherheitsanforderungen

6.1. Hinweise und Definitionen

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

6.1.1. Hinweise zur Notation

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-0098] 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

6.1.2.1. Hinweise zu Übernahmen aus dem Schutzprofil

Die Architektur des TOE mit seinen Java Virtual Machines ist monolithischer als es die Definitionen der Subjekte im Schutzprofil suggerieren. Die dort definierten Subjekte wie S_AK, S_Signaturdienst, S_Chipkartendienst etc. sind grundsätzlich auch für die KoCoBox MED+ anwendbar. Jedoch manifestieren sie sich *nicht* in der Implementierung in Form von separaten Prozessen. Alle diese Subjekte existieren in der JVM des Anwendungskonnektors. Innerhalb der JVM sind die Subjekte nicht physisch voneinander abgegrenzt. Das hat Implikationen auf die Sicherheitsanforderungen in den Familien FDP_ACC und FDP_ACF. Anforderungen wie „Nur der Chipkartendienst darf…“ werden nicht durch Kontrollmechanismen umgesetzt, sondern dadurch, dass aus der Implementierung heraus ersichtlich ist, dass keine Aufrufe stattfinden, die nicht in der Sicherheitsarchitektur vorgesehen sind.

6.2. Funktionale Sicherheitsanforderungen des Netzkonnektors

6.2.1. VPN Client

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

FTP_ITC.1.1/NK.VPN_TI	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.
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].

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

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,

(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:

[11] Assignment: *information flow control SFP*
[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*

(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).

(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.

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

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

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

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

(7) The TSF shall allow

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

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

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

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

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

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

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

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

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

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

(9) The TSF shall allow

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

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

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

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

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

b) The rules ANLW_FW_SIS_ADMIN_RULES applies if defined.

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

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

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

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:

(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

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

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

(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]

[20] Assignment: *Additional rules, based on security attributes, that explicitly deny information flows*

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.

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.

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

ST-Anwendungshinweis 5

Das Schutzprofil fordert in Anwendungshinweis 87, dass die „Korrektheit der Kommunikation zwischen dem NK und anderen Konnektorteilen“ im Rahmen der Prüfung von FPT_STM.1/NK evaluiert wird. Aus diesem Grund werden Module der Subsysteme 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.

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].

[26] Assignment: *list of TSF data types*
[27] Assignment: *list of interpretation rules to be applied by the TSF*
[28] Refinement: *Gemäß Vorgaben aus A_21185*

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].
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.

[29] Assignment: *list of objects*
[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*

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],

(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-0098]**

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

[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)*
[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*

- 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:

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

[46] Assignment: *other specifically defined auditable events*
[47] Assignment: *other audit relevant information*

- 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.

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.**

[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)*
[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*

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]
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.

[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]*
[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*

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.

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].

[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*

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 sha256with-RSAEncryption OID 1.2.840.113549.1.1.11 **, ecdsa-with-SHA256 OID 1.2.840.10045.4.3.2 with curves brainpoolP256r1**[67] and 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**

[65] Refinement: *Gemäß Vorgaben aus A_17125*
[66] Assignment: *list of cryptographic operations*
[67] Assignment: *cryptographic algorithm*
[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*

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 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.

[76] Assignment: *cryptographic key sizes*
[77] Assignment: *list of standards*
[78] Assignment: *cryptographic key generation algorithm*
[79] Assignment: *cryptographic key sizes*

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].

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-0098] gilt ohne Einschränkungen. Die umgesetzten Cipher Suiten aus dem Schutzprofil und der gematik Spezifikation [gemSpec_Krypt] werden in Tabelle B.1 auf Seite 228 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.

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

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

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

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

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

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

(4) importierte X.509 Zertifikate für Clientsysteme

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

(6) 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,

[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*

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 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 follo-

[92] Refinement: *Gemäß Vorgaben aus A_17094-01, A_17124-01*
[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*

wing: 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 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,

[104] Assignment: *list of standards*
[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

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.

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.

[113] Refinement: *Die Quelle für den PKCS#12 Standard wurde gegenüber dem Schutzprofil aktualisiert.*
[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)*

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

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

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

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

(2) Die TSF importiert X.509 Zertifikate und 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]

[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*

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:

(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]

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

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 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.

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

(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 $w > 1 - 2^{(-16)}$.

(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].

[123] Assignment: *a defined quality metric*
[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].

6.3. Funktionale Sicherheitsanforderungen des Anwendungskonnektors

6.3.1. Klasse FCS: Kryptographische Unterstützung

6.3.1.1. Basisalgorithmen

Der Konnektor nutzt kryptographische Dienste der gSMC-K in der Einsatzumgebung. Das Schutzprofil COS [BSI-CC-PP-0082-2] fordert die Evaluierung der kryptographischen Funktionen des Betriebssystems der gSMC-K, die durch das Objektsystem der gSMC-K ausgewählt werden.

6.3.1.2. Schlüsselerzeugung und Schlüssellöschung

FCS_COP.1/AK.SHA
Cryptographic operation / hash value calculation AK

FCS_COP.1.1/AK.SHA	The TSF shall perform hash value calculation[132] in accordance with a specified cryptographic algorithm SHA-256, SHA-384 und SHA-512[133] and cryptographic key sizes none[134] that meet the following: Standard FIPS PUB 180-4 [FIPS 180-4].

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

FCS_CKM.1/AK.AES

Cryptographic key generation / AES keys

FCS_CKM.1.1/AK.AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm randomly created according to FCS_RNG.1/Hash_DRBG[135] and specified cryptographic key sizes 256 bit that meet the following: NIST-SP800-133 [NIST SP 800-133, Section 6.1][136].

FCS_CKM.4/AK

Cryptographic key destruction

FCS_CKM.4.1/AK	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwrite with constant values[137] that meet the following none[138].

6.3.1.3. Signaturerzeugung und Signaturprüfung

FCS_COP.1/AK.SigVer.SSA

Cryptographic operation / Signature verification PKCS#1 SSA

FCS_COP.1.1/AK.SigVer.SSA	The TSF shall perform verification of digital signatures in accordance with a specified cryptographic algorithm RSASSA-PKCS1-v1_5 signature verification and cryptographic key sizes ~~1976 bit to 4096 bit~~ **1900 bit to 8192 bit** that meet the following: Standard PKCS#1 [RFC 8017].

FCS_COP.1/AK.SigVer.PSS

Cryptographic operation / Signature verification PKCS#1 PSS

FCS_COP.1.1/AK.SigVer.PSS	The TSF shall perform verification of digital signatures in accordance with a specified cryptographic algorithm RSASSA-PSS signature verification and cryptographic key sizes ~~1976 bit to 4096 bit~~ **1900 bit to 8192 bit** that meet the following: Standard PKCS#1 v2.2 [RFC 8017].

FCS_COP.1/AK.SigVer.ECDSA

Cryptographic operation / Signature verification ECDSA

FCS_COP.1.1/AK.SigVer.ECDSA	The TSF shall perform verification of digital signatures in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 256**, 384, and 512** bit that meet the following: Standard TR-03111 [TR-03111].

[135] Assignment: *Algorithm for cryptographic key generation of AES keys*
[136] Assignment: *list of standards*
[137] Assignment: *cryptographic key destruction method*
[138] Assignment: *list of standards*

FCS_COP.1/AK.XML.Sign

Cryptographic operation / XML signature generation

FCS_COP.1.1/AK.XML.Sign

The TSF shall perform the generation of XML-signed documents **and XML-signed SAML2 assertions** **with digital signatures created from signature smartcards** in accordance with a specified cryptographic algorithm

(1) XML Advanced Electronic Signature (XAdES),

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

and cryptographic key sizes no key that meet the following: Standards XMLSig [XMLSig2], XAdES [XAdES; XAdES-BL] and FIPS PUB 180-4 [FIPS 180-4], **SAML2 [SAML2.0]**.

FCS_COP.1/AK.CMS.Sign

Cryptographic operation / CMS signature generation

FCS_COP.1.1/AK.CMS.Sign

The TSF shall perform sign documents with digital signatures created from signature smartcards[139] in accordance with a specified cryptographic algorithm

(1) CMS Advanced Electronic Signature (CAdES),

(2) SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS[140]

and cryptographic key sizes no key[141] that meet the following: Standards RFC 5652 [RFC 5652], CAdES [CAdES; CAdES-BL] and FIPS PUB 180-4 [FIPS 180-4].

FCS_COP.1/AK.PDF.Sign

Cryptographic operation / PDF signature generation

FCS_COP.1.1/AK.PDF.Sign

The TSF shall perform sign PDF-A documents[142] **with digital signatures created from signature smartcards**[143] in accordance with a specified cryptographic algorithm SHA-256 according to FCS_COP.1/AK.SHA for the creation of the DTBS[144] and cryptographic key sizes no key[145] that meet the following: Standards PAdES [PAdES; PAdES-BL] and FIPS PUB 180-4 [FIPS 180-4][146].

[139] Assignment: *list of cryptographic operations*
[140] Assignment: *cryptographic algorithm*
[141] Assignment: *cryptographic key sizes*
[142] Assignment: *list of cryptographic operations*
[143] Refinement
[144] Assignment: *cryptographic algorithm*
[145] Assignment: *cryptographic key sizes*
[146] Assignment: *list of standards*

FCS_COP.1/AK.XML.SigPr

Cryptographic operation / XML Signature verification

FCS_COP.1.1/AK.XML.SigPr

The TSF shall perform verify signed XML documents in accordance with a specified cryptographic algorithm

(1) XML Advanced Electronic Signature (XAdES),

(2) SHA-256, SHA-384 and SHA-512 for QES according to FCS_COP.1/AK.SHA with

RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,

RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES

and cryptographic key sizes ~~1976 bit to 4096 bit~~ **1900 bit to 8192 bit** for QES,

(3) SHA-256**, SHA-384, and SHA-512** with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA and cryptographic key sizes 256**, 384, and 512** bit for QES that meet the following: Standards XMLSig [XMLSig2], XAdES [XAdES; XAdES-BL], FIPS PUB 180-4 [FIPS 180-4], PKCS#1 [RFC 8017] and TR-03111 [TR-03111].

FCS_COP.1/AK.CMS.SigPr

Cryptographic operation / CMS Signature verification

FCS_COP.1.1/AK.CMS.SigPr

The TSF shall perform verify signed CMS documents in accordance with a specified cryptographic algorithm

(1) CMS Advanced Electronic Signature (CAdES),

(2) SHA-256, SHA-384 and SHA-512 for QES and SHA-256 for nonQES according to FCS_COP.1/AK.SHA with

RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,

RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES and nonQES

and cryptographic key sizes ~~1976 bit to 4096 bit~~ **1900 bit to 8192 bit** for QES and 2048 bit **to 8192 bit** for nonQES,

(3) SHA-256**, SHA-384, and SHA-512** with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA and cryptographic key sizes 256**, 384, and 512** bit for QES and nonQES that meet the following: Standards RFC 5652 [RFC 5652], CAdES [CAdES; CAdES-BL], FIPS PUB 180-4 [FIPS 180-4], PKCS#1 [RFC 8017] and TR-03111 [TR-03111].

FCS_COP.1/AK.PDF.SigPr

Cryptographic operation / PDF Signature verification

FCS_COP.1.1/AK.PDF.SigPr The TSF shall perform verify signed PDF-A documents in accordance with a specified cryptographic algorithm

(1) PAdES [PAdES; PAdES-BL],

(2) SHA-256, SHA-384 and SHA-512 for QES and SHA-256 for nonQES according to FCS_COP.1/AK.SHA with

RSA with PKCS#1 SSA-V1.5 according to FCS_COP.1/AK.SigVer.SSA for QES,

RSA with PKCS#1 PSS according to FCS_COP.1/AK.SigVer.PSS for QES and nonQES

and cryptographic key sizes ~~**1976 bit to 4096 bit**~~ **1900 bit to 8192 bit** for QES and 2048 bit **to 8192 bit** for nonQES,

(3) SHA-256**, SHA-384, and SHA-512** with ECDSA according to FCS_COP.1/AK.SigVer.ECDSA and cryptographic key sizes 256**, 384, and 512** bit for QES and nonQES that meet the following: Standards PAdES [PAdES; PAdES-BL], FIPS PUB 180-4 [FIPS 180-4], PKCS#1 [RFC 8017] and TR-03111 [TR-03111]

FCS_COP.1/AK.SigVer.BNetzA-VL

Cryptographic operation / Signature verification of BNetzA-VL

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
hier erfüllt durch: FDP_ITC.2/AK.BNetzA-VL

FCS_CKM.4 Cryptographic key destruction
hier erfüllt durch: FCS_CKM.4/AK

FCS_COP.1.1/AK.SigVer.BNetzA-VL The TSF shall perform signature verification of BNetzA-VL[147] in accordance with a specified cryptographic algorithm according to column 1 of Tabelle 6.4[148] and cryptographic key sizes according to column 2 of Tabelle 6.4[149] that meet the following: PKCS#1 [RFC 8017], FIPS PUB 186-4 [FIPS 186-4], RFC 5639 [RFC 5639] and FIPS PUB 180-4 [FIPS 180-4][150].

[147] Assignment: *list of cryptographic operations*
[148] Assignment: *cryptographic algorithm*
[149] Assignment: *cryptographic key sizes*
[150] Assignment: *list of standards*

Algorithm	Key size (bits)/Curve
RSASSA-PSS w/ SHA256/-384/-512	1900 – 8192
RSASSA-PKCS1-v1_5 w/ SHA256	1900 – 8192
RSASSA-PKCS1-v1_5 w/ SHA384	1900 – 8192
RSASSA-PKCS1-v1_5 w/ SHA512	1900 – 8192
ECDSA w/ SHA256	brainpoolP256r1
ECDSA w/ SHA384	brainpoolP384r1
ECDSA w/ SHA512	brainpoolP512r1

Tabelle 6.4.: Algorithms, Key sizes/Curve of Signature Verification of BNetzA-VL

6.3.1.4. Ver- und Entschlüsselung von Dokumenten

FCS_COP.1/AK.AES

Cryptographic operation / AES encryption and decryption

FCS_COP.1.1/AK.AES	The TSF shall perform symmetric encryption and decryption[151] in accordance with a specified cryptographic algorithm AES-GCM[152] and cryptographic key sizes 128 bit, 192 bit and 256 bit[153] **and 96 bit initialization vector created by secure RNG according to FCS_RNG.1/Hash_DRBG**[154] that meet the following: Standards FIPS PUB 197 [FIPS 197], NIST-SP800-38A [NIST SP 800-38A][155].
ST-Anwendungshinweis 21	Die Schlüssellängen 128 bit und 192 bit kommen ausschließlich bei der Entschlüsselung zur Anwendung. Der TOE verschlüsselt immer mit 256 bit, vgl. die Schlüsselgenerierung in FCS_CKM.1/AK.AES.

FCS_COP.1/AK.ECIES

Cryptographic operation / ECIES encryption

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FDP_ITC.2/AK.Enc, FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/AK.ECIES	The TSF shall perform ECIES-based authenticated hybrid encryption[156] in accordance with a specified cryptographic algorithm ECIES

[151] Assignment: *list of cryptographic operations*
[152] Assignment: *cryptographic algorithm*
[153] Assignment: *cryptographic key sizes*
[154] Refinement: *Gemäß Vorgaben aus GS-A_5016*
[155] Assignment: *list of standards*
[156] Assignment: *list of cryptographic operations* / Gemäß Vorgaben aus A_17220

with ECKA based on brainpoolP256r1, KDF with SHA-256, AES-CBC-256, and CMAC[157] and cryptographic key sizes 256 bit for ECKA, KDF and AES-CBC[158] **and 8 Byte CMAC tag length** that meet the following:

ECIES	SEC 1: Elliptic Curve Cryptography [SEC1-2009], gematik spec. [gemSpec_Krypt],
brainpoolP256r1	RFC 5639 [RFC 5639],
ECKA	TR-03111 [TR-03111, Section 4.3.1],
KDF	TR-03110-3 [TR-03110-3, Section A.2.3.2],
SHA-256	FIPS PUB 180-4 [FIPS 180-4],
AES	FIPS PUB 197 [FIPS 197],
CBC	NIST-SP800-38A [NIST SP 800-38A],
CMAC	NIST-SP800-38B [NIST SP 800-38B]

[159].

ST-Anwendungshinweis 22

Der TOE setzt nur die Verschlüsselung um, die Entschlüsselung wird von der beteiligten Chipkarte durchgeführt.

Den *öffentlichen Schlüssel des Empfängers* für das hybride ECIES-Verfahren erhält der TOE beim Aufruf des Verschlüsselungsdienstes via SOAP an der Außenschnittstelle LS.LAN.EncryptionService durch das Clientsystem. Dieser SOAP-Request enthält das Zertifikat des Empfängers. Der Import der Daten beim Aufruf des Verschlüsselungsdienstes ist durch das Schutzprofil in FDP_ITC.2/AK.Enc modelliert.

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

FCS_COP.1.1/AK.XML.Ver

The TSF shall perform encryption of XML documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm RSA RSAOAEP and AES-GCM with authentication tag length of 128 bit **and 96 bit initialization vector created by secure RNG according to FCS_RNG.1/Hash_DRBG**[160] and cryptographic key sizes 256 bit for AES and 2048 bit **to 8192 bit** for RSA that meet the following: Standards NIST-SP800-38D [NIST SP 800-38D], PKCS#1 [RFC 8017], FIPS PUB 197 [FIPS 197] und XMLEnc [XMLEnc].

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

FCS_COP.1.1/AK.XML.Ent

The TSF shall perform decryption of XML documents in a hybrid cryptosystem in accordance with a specified cryptographic al-

[157] Assignment: *cryptographic algorithm*
[158] Assignment: *cryptographic key sizes*
[159] Assignment: *list of standards*
[160] Refinement: *Gemäß Vorgaben aus GS-A_5016*

gorithm *RSAOAEP*[161] and AES-GCM with authentication tag length of 128 bit and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST-SP800-38D [NIST SP 800-38D], FIPS PUB 197 [FIPS 197] and XMLEnc [XMLEnc].

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

FCS_COP.1.1/AK.CMS.Ver

The TSF shall perform encryption of documents in a hybrid cryptosystem in accordance with a specified cryptographic algorithm RSA RSAOAEP **or ECIES for the asymmetric operation**[162] and AES-GCM with authentication tag length of 128 bit **and 96 bit initialization vector created by secure RNG according to FCS_RNG.1/Hash_DRBG**[163] **for the symmetric operation** and cryptographic key sizes 256 bit for AES and 2048 bit **to 8192 bit** for RSA **and 256 bit for ECIES** that meet the following: Standards NIST-SP800-38D [NIST SP 800-38D], PKCS#1 [RFC 8017], FIPS PUB 197 [FIPS 197], and CMS [RFC 5652] **and gematik specification [gemSpec_Krypt, Section 5.7]**.

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

FCS_COP.1.1/AK.CMS.Ent

The TSF shall perform decryption of documents in accordance with a specified cryptographic algorithm *RSAOAEP*[164] **or ECIES for the asymmetric operation**[165] and AES-GCM with authentication tag length of 128 bit **for the symmetric operation** and cryptographic key sizes 128 bit, 192 bit and 256 bit that meet the following: Standards NIST-SP800-38D [NIST SP 800-38D], PKCS#1 [RFC 8017], FIPS PUB 197 [FIPS 197] and CMS [RFC 5652] **and gematik specification [gemSpec_Krypt, Section 5.7]**.

6.3.2. Klasse FIA: Identifikation und Autorisierung

FIA_SOS.1/AK.Passwörter
Verification of secrets / Passwords

FIA_SOS.1.1/AK.Passwörter

The TSF shall provide a mechanism to verify that **administrator passwords**[166] meet the following criteria:

- A password consists of the following character classes: uppercase letters, lowercase letters, special characters and numbers.

[161] Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP*
[162] Refinement: *Gemäß Vorgaben aus A_17220*
[163] Refinement: *Gemäß Vorgaben aus GS-A_5016*
[164] Selection: *RSA RSAES-PKCS1-v1_5, RSAOAEP*
[165] Refinement: *Gemäß Vorgaben aus A_17220*
[166] Refinement

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

[167] .

ST-Anwendungshinweis 23

Die Zuweisungen in diesem SFR setzen die Anforderungen aus TIP1-A_4808-01 um.

Die Eingabe einer ungültige Kombination aus Benutzernamen und Passwort erzwingt eine Pause von 3 Sekunden vor der nächsten Eingabemöglichkeit. Nach dem dritten aufeinander folgenden fehlgeschlagenen Anmeldeversuch desselben Benutzers wird der Benutzer für 60 Sekunden gesperrt. Jeder weitere Fehlversuch führt zu einer erneuten Sperre von 60 Sekunden (siehe Unterabschnitt 7.2.3).

FIA_SOS.1/AK.CS.Passwörter

Verification of secrets / Passwords for client systems

FIA_SOS.1.1/AK.CS.Passwörter

The TSF shall provide a mechanism to verify that passwords for client systems meet the following criteria: A password consists of the following character classes: uppercase letters, lowercase letters, numbers, space and the following characters: `!@#$%^&*=+-/.` [168]

ST-Anwendungshinweis 24

Das verfügbare Alphabet umfasst 75 Zeichen. Bei einer Länge von 17 Zeichen ergibt sich eine Entropie von >105 Bit für ein zufällig gewähltes Passwort des Nutzers. Der Hersteller sieht dies als ausreichend sicher an.

Um die Interoperabilität mit Clientsystemen zu wahren, werden auch Passwörter mit mindestens 6 Zeichen Länge akzeptiert. Wenn das Passwort kürzer als 17 Zeichen ist, erscheint eine Warnung. Darüber hinaus erhält der Dialog die Möglichkeit zur Generierung eines sicheren Passworts mit 20 Zeichen (Sicherheitsniveau 120 Bit). Als Quelle für dieses Passwort wird der gSMC-K-basierte Zufallsgenerator herangezogen.

Nach einem fehlgeschlagenen Authentisierungsversuch wird eine Sperre von 3 Sekunden für das Clientsystem verhängt (siehe Unterabschnitt 7.2.3).

[167] Assignment: *a defined quality metric*
[168] Assignment: *a defined quality metric*

FIA_SOS.2/AK.PairG
Generation of pairing secrets

FIA_SOS.2.1/AK.PairG — The TSF shall provide a mechanism to generate **pairing**[169] secrets that meet the requirement to consist of 16 random bytes with 100 bit of entropy[170].

FIA_SOS.2.2/AK.PairG — The TSF shall be able to enforce the use of TSF generated **pairing**[171] secrets for authentication of eHealth cardterminals[172].

FIA_UID.1/AK
Timing of identification

FIA_UID.1.1/AK — The TSF shall allow

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

(2) no further action[173]

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

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

FIA_UAU.1/AK
Timing of authentication

FIA_UAU.1.1/AK — The TSF shall allow

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

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

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

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

(5) no further action.[174]

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

FIA_UAU.1.2/AK — The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[169] Refinement
[170] Assignment: *a defined quality metric*
[171] Refinement
[172] Assignment: *list of TSF functions*
[173] Assignment: *list of TSF-mediated actions*
[174] Assignment: *list of TSF mediated actions*

FIA_UAU.5/AK
Multiple authentication mechanisms

FIA_UAU.5.1/AK

The TSF shall provide

(1) *password based authentication mechanism*[175] for administrator users,

(2) TLS authentication with a pairing secret for eHKT [gemSpec_Kon], TUC_KON_050,

(3) Asymmetric authentication of a smart card including CVC verification without negotiation of symmetric keys,

(4) Mutual asymmetric authentication with a smart card with CVC verification and negotiation of symmetric keys for a secure messaging channel,

(5) password based and certificate based authentication mechanisms for client systems,[176]

(6) User ID based authentication mechanism for Komfortsignatur with the User ID being a UUID according to RFC 4122 [RFC 4122] of length 128 bit that must be unique with respect to the last 1000 activations[177]

to support user authentication.

ST-Anwendungshinweis 25

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

TLS-Handshake und Verwendung des Pairing-Geheimnisses geschehen jedoch auf unterschiedlichen Ebenen des Protokollstapels. Somit kann das Pairing-Geheimnis nicht in die Authentisierung im TLS-Handshake verwendet werden.

Gemäß A_22458 darf der Konnektor für die TLS-Verbindung zu einem Kartenterminal ausschließlich die Cipher-Suite anbieten, die beim Pairing mit genau diesem Kartenterminal verwendet wurde. Insofern ergibt sich eine Kopplung aus TLS-Handshake und Pairing-Geheimnis. Wir interpretieren die Formulierung im SFR im Einklang mit der Anforderung A_22458.

ST-Anwendungshinweis 26

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

[175] Selection: *password based authentication mechanism, [another authentication mechanism]*
[176] Refinement: *Gemäß Vorgaben aus TIP1-A_4516*
[177] Refinement: *Gemäß Vorgaben aus A_20073-01, A_20074*

ST-Anwendungshinweis 27 — Unterpunkt (6): Die User ID wird vom Clientsystem generiert. Das Clientsystem garantiert ausreichenden Zufall bei der Generierung der User ID.

FIA_UAU.5.2/AK — The TSF shall authenticate any user's claimed identity according to the following rules:

(1) The TSF shall authenticate the user for all administration functions.

(2) The TSF shall authenticate eHealth card terminals when establishing the TLS channel between the TSF and the eHealth card terminal.

(3) The TSF shall support the authentication of a eGK (identified by the ICCSN) with its smart card certificate.

(4) The TSF shall authenticate the HBA for a batch signature:

a) as a QSEE,

b) as a DTBS and PIN receiver before a signature creation process with negotiating symmetric keys for a secure messaging channel,

c) constantly during the signature process with secure messaging.

(5) The TSF shall authenticate the HBA before a single signature creation within the card session.

(6) The TSF shall support mutual authentication in a remote PIN process: The gSMC-KT in the role of the PIN transmitter and the HBA (or the SMC-B) in the role of the PIN receiver[178].

FIA_API.1/AK
Authentication Proof of Identity

FIA_API.1.1/AK — The TSF shall provide a card-to-card authentication mechanism with key derivation for secure messaging[179] to prove the identity of the "SAK"[180].

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

FIA_API.1.1/AK.TLS — The TSF shall provide a TLS authentication mechanism using a certificate from the list in FMT_MOF.1.1/NK.TLS(10)[181] to prove the identity of the TOE[182].

[178] Assignment: *rules describing how the multiple authentication mechanisms provide authentication*
[179] Assignment: *authentication mechanism*
[180] Assignment: *identity or role*
[181] Assignment: *authentication mechanism*
[182] Assignment: *identity or role*

ST-Anwendungshinweis 28 Eigenes SFR hinzugefügt auf Basis der Anforderung GS-A_4384-01.

6.3.3. Klasse FDP: Schutz der Benutzerdaten

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

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

6.3.3.1. Zugriffskontrolldienst

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

FDP_ACC.1.1/AK.Infomod — The TSF shall enforce the Infomodell-SFP[183] on the subject S_Clientsystem, the objects as in TAB_KON_507, and the operation:

- usage of the resource (the object) in a technical use case[184].

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

FDP_ACF.1.1/AK.Infomod — The TSF shall enforce the Infomodell-SFP[185] to objects based on the following:

the subject S_Clientsystem with its associated security attributes defined in Tabelle 12, and the objects with their associated security attributes defined in TAB_KON_508 and TAB_KON_509[186].

FDP_ACF.1.2/AK.Infomod — The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: TAB_KON_511, TAB_KON_512, TAB_KON_513 and TAB_KON_514[187].

FDP_ACF.1.3/AK.Infomod — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[188].

[183] Assignment: *access control SFP*
[184] Assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*
[185] Assignment: *access control SFP*
[186] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*
[187] Assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
[188] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*

FDP_ACF.1.4/AK.Infomod — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[189].

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

FMT_MSA.1.1/AK.Infomod — The TSF shall enforce the Infomodell-SFP[190] to restrict the ability to *modify, delete, create*[191] the security attributes persistent entities and entity-connections defined in TAB_KON_507, TAB_KON_508, TAB_KON_509 according to the contraints in TAB_KON_510[192] to S_Administrator[193].

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

FMT_MSA.3.1/AK.Infomod — The TSF shall enforce the Infomodell-SFP to provide *no*[194] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/AK.Infomod — The TSF shall allow the *no role*[195] to specify alternative initial values to override the default values when an object or information is created.

ST-Anwendungshinweis 29 — Es gibt keine vom Administrator überschreibbaren Konfigurationswerte. Folglich gibt es auch keine alternativen Anfangswerte. Die Anforderung ist implizit erfüllt.

6.3.3.2. Kartenterminaldienst

FDP_ACC.1/AK.eHKT
Subset access control / Kartenterminaldienst

FDP_ACC.1.1/AK.eHKT — The TSF shall enforce the Kartenterminaldienst-SFP[196] on subjects:

(1) S_Kartenterminaldienst,
(2) S_Chipkartendienst,
(3) S_Verschlüsselungsdienst,
(4) S_AK,
(5) S_eHKT,

[189] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*
[190] Assignment: *access control SFP(s), information flow control SFP(s)*
[191] Selection: *change_default, , query, modify, delete, [assignment: other operations]*
[192] Assignment: *list of security attributes*
[193] Assignment: *the authorised identified roles*
[194] Selection: *selection, choose one of: restrictive, permissive, [assignment: other property]*
[195] Selection: *S_Administrator, no role*
[196] Assignment: *access control SFP*

(6) S_Fachmodul,

(7) S_Clientsystem;

objects:

(1) eHealth-Kartenterminal,

(2) TLS-Kanal,

(3) SICCT-Kommando,

(4) Antwort auf SICCT-Kommando,

(5) Eingeschränkter Text;

operations:

(1) TLS-Kanal aufbauen,

(2) TLS-Kanal abbauen,

(3) Senden eines SICCT-Kommando anfordern,

(4) SICCT-Kommando senden,

(5) Antwort auf SICCT-Kommando empfangen;[197]

.

FDP_ACF.1/AK.eHKT
Security attribute based access control / Kartenterminaldienst

FDP_ACF.1.1/AK.eHKT The TSF shall enforce the Kartenterminaldienst-SFP[198] to objects based on the following: list of subjects, objects and security attributes:

subjects:

(1) S_Kartenterminaldienst,

(2) S_Chipkartendienst,

(3) S_Signaturdienst

(4) S_Verschlüsselungsdienst,

(5) S_AK with the security attributes:

a) “Aufrufender: Clientsystem”,

b) “Aufrufender: Fachmodul”

(6) S_eHKT,

(7) S_Fachmodul,

(8) S_Clientsystem;

objects:

(1) eHealth-Kartenterminal with security attribute „Arbeitsplatz“,

(2) TLS-Kanal

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

[198] Assignment: *access control SFP*

(3) SICCT-Kommando with security attribute „Typ des SICCT-Kommandos“,

(4) Antwort auf SICCT-Kommando[199]

.

FDP_ACF.1.2/AK.eHKT

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Only the Kartenterminaldienst may establish TLS-Kanäle to paired eHealth-Kartenterminals with mutual authentication.

(2) Only the Kartenterminaldienst may shutdown TLS-Kanäle to eHealth-Kartenterminals. This is only allowed in case that communication errors have been detected.

(3) Only the Kartenterminaldienst may send SICCT-Kommandos and receive the associated reponses, which are used to control the eHealth-Kartenterminals (eHKT-Steuerungskommando).

(4) Only the Kartenterminaldienst and the Chipkartendienst may send SICCT-Kommandos and receive the associated reponses, which are used to access the secure display and the PIN pad of the eHealth-Kartenterminals (Benutzerkommuikationskommando).

(5) The subject S_AK, calling subject = Fachmodul may

- pass SICCT-Kommandos to the Kartenterminaldienst which are used to display eingeschränkten Text on a identified eHealth-Kartenterminal and
- receive the associated reponses to the SICCT-Kommandos from the Chipkartendienst.

(6) Only the Chipkartendienst, the Signaturdienst and the Verschlüsselungsdienst may send SICCT-Kommandos via the TLS-Kanäle of the Kartenterminaldienst and receive the associated reponses, which are used to access inserted smart cards (Chipkartenkommando).

(7) Only the Chipkartendienst may send SICCT-Kommandos and receive the associated reponses, which are used for PIN entry, PUK entry and PIN change use cases in secure mode at the eHealth-Kartenterminals (PIN-Prozesskommando).

(8) Fachmodule and Clientsysteme may register themselves for the events „smart card inserted“ and „smart card removed“, to be notified if the events occur.[200]

[199] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

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

.

FDP_ACF.1.3/AK.eHKT — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: The S_Kartenterminaldienst may establish a communication channel to an unpaired eHealth-Kartenterminal for the purpose of setup and pairing.[201]

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

(1) Only the subject S_Chipkartendienst may send a SICCT-Kommando via the TLS-Kanal of the TOE to the eHealth-Kartenterminal, which is used to display the messages Signatur PIN, Signatur PUK, Freigabe PIN, Praxis PIN, Freigabe PUK oder Praxis PUK at the eHealth-Kartenterminals.

(2) The subject S_Kartenterminaldienst must not send SICCT or EHEALTH-Commands to a card terminal for which *CT.CONNECTED=Nein* is set, with the exception of the commands listed in TAB_KON_785 [gemSpec_Kon].[202]

ST-Anwendungshinweis 30 — Die zusätzliche Regel in FDP_ACF.1.4/AK.eHKT(2) greift die Anforderung TIP1-A_6478 der Konnektor-Spezifikation auf.

FDP_UCT.1/AK.TLS

Basic data exchange confidentiality

FDP_UCT.1.1/AK.TLS — The TSF shall enforce the Kartenterminaldienst-SFP[203] to *transmit and receive*[204] ~~**user data**~~ **objects**[205] in a manner protected from unauthorised disclosure.

FDP_UIT.1/AK.TLS

Basic data exchange integrity

FDP_UIT.1.1/AK.TLS — The TSF shall enforce the Kartenterminaldienst-SFP[206] to *transmit and receive*[207] user data ~~**in a manner**~~ protected from *modification, deletion, insertion, replay*[208] errors.

FDP_UIT.1.2/AK.TLS — The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, replay*[209] has occurred.

[201] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[202] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[203] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[204] Selection: *transmit, receive*
[205] Refinement
[206] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[207] Selection: *transmit, receive*
[208] Selection: *modification, deletion, insertion, replay*
[209] Selection: *modification, deletion, insertion, replay*

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

FMT_MTD.1.1/AK.eHKT_Abf

The TSF shall restrict the ability to *query and export*[210] the Arbeitsplatzkonfigurationsdaten:

(1) Name eines zugelassenen eHealth-Kartenterminals,

(2) Statische IP-Adresse eines Kartenterminals,

(3) Konfiguration des SICCT-Kommandointerpreter Ports eines eHealth-Kartenterminals,

(4) Authentisierungsreferenzdaten mit Identität und Zertifikat der zugelassenen eHealth-Kartenterminals,

(5) Zuordnung eines eHealth-Kartenterminals zum Arbeitsplatz,

(6) Export von eHealth-Kartenterminal-Informationen

:[211]

to S_AK and S_Administrator[212].

Pairing-Geheimnisse dürfen nur unter Wahrung der Vertraulichkeit exportiert und dürfen nicht abgefragt werden.[213]

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

FMT_MTD.1.1/AK.eHKT_Mod

The TSF shall restrict the ability to *modify, delete and import*[214] the Arbeitsplatzkonfigurationsdaten:

(1) Name eines zugelassenen eHealth-Kartenterminals,

(2) Statische IP-Adresse eines zugelassenen eHealth- Kartenterminals,

(3) Konfiguration des SICCT-Kommandointerpreter Ports eines eHealth-Kartenterminals,

(4) Authentisierungsreferenzdaten mit Identität und Zertifikat der zugelassenen eHealth-Kartenterminals,

(5) Zuordnung eines eHealth-Kartenterminals zum Arbeitsplatz

(6) Import von eHealth-Kartenterminal-Informationen nach Anzeige und Bestätigung

:[215]

to S_Administrator[216].

[210] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[211] Assignment: *list of TSF data*
[212] Assignment: *the authorised identified roles*
[213] Refinement
[214] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[215] Assignment: *list of TSF data*
[216] Assignment: *the authorised identified roles*

6.3.3.3. Chipkartendienst

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

FDP_ACC.1.1/AK.KD The TSF shall enforce the Chipkartendienst-SFP[217] on

subjects:

(1) S_Chipkartendienst,

(2) S_Signaturdienst,

(3) S_Verschlüsselungsdienst,

(4) S_AK,

(5) S_Fachmodul,

(6) S_Clientsystem;

objects:

(1) Chipkarte,

(2) Logischer Kanal einer Chipkarte,

(3) SICCT-Kommando with security attribute „Chipkartenkommando";

operations:

(1) Kartenhandle ausgeben,

(2) logischen Kanal anfordern,

(3) logischen Kanal öffnen,

(4) logischen Kanal schließen,

(5) die Card-to-card-Authentisierung anfordern,

(6) die Card-to-card-Authentisierung durchführen,

(7) Digitale Signatur erstellen,

(8) Chiffrate entschlüsseln,

(9) auf Kartenobjekte zugreifen,

(10) Chipkartenkommando übertragen und Antwort empfangen,

(11) Benutzerauthentisierung anforndern

.[218]

[217] Assignment: *access control SFP*

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

FDP_ACF.1/AK.KD

Security attribute based access control / Chipkartendienst

FDP_ACF.1.1/AK.KD

The TSF shall enforce the Chipkartendienst-SFP[219] to objects based on the following: list of subjects, objects and security attributes:

subjects:

(1) S_Chipkartendienst,

(2) S_Signaturdienst,

(3) S_Verschlüsselungsdienst,

(4) S_AK,

(5) S_Fachmodul,

(6) S_Clientsytem

objects:

(1) Chipkarte with security attributtes:

a) „Kartentyp“,

b) „Kartenhandle“,

(2) Logischer Kanal einer Chipkarte with security attribute „Sicherheitszustand“,

(3) SICCT-Kommando with security attribute „Chipkartenkommando”

:[220]

FDP_ACF.1.2/AK.KD

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Der S_Chipkartendienst erzeugt für jede neu gesteckte Chipkarte ein Kartenhandle und übergibt für identifizierte eGK, SMC-B und HBA den im gespeicherten X.509 angegeben Namen des Kartenhalters an das Subjekt S_AK.

(2) Die Subjekte S_AK und S_Fachmodul dürfen einen neu zu öffnenden logischen Kanal einer mit dem Kartenhandle identifizierten Chipkarte mit ggf. identifizierten User-ID, Clientsystem-ID, Arbeitsplatz anfordern. Wenn die übergebenen Identitäten mit der Arbeitsplatzkonfiguration konsistent sind und die identifizierte Chipkarte einen logischen Kanal bereitstellt, öffnet der Chipkartendienst einen solchen logischen Kanal und erlaubt den Zugriff auf die Chipkarte, wenn dem keine andere Zugriffsregel widerspricht

[219] Assignment: *access control SFP*

[220] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

(3) Der Signaturdienst und der Verschlüsselungsdienst dürfen einen neu zu öffnenden logischen Kanal einer mit dem Kartenhandle identifizierten Chipkarte anfordern. Wenn die identifizierte Chipkarte einen logischen Kanal bereitstellt, öffnet der Chipkartendienst einen solchen logischen Kanal.

(4) Nur die Subjekte S_AK, S_Signaturdienst und S_Fachmodul dürfen die Card-to-Card- Authentisierung zwischen zwei logischen Kanäle verschiedener Chipkarten anfordern. Nur das Subjekt Chipkartendienst darf die Card-to-Card- Authentisierung für logische Kanäle durchführen.

(5) Nur der Signaturdienst darf mit den Chipkarten digitale Signaturen für QES und nonQES mit den Kommandos MANAGE SECURITY ENVIRONMENT und PSO COMPUTE DIGITAL SIGNATURE erzeugen.

(6) Nur der Verschlüsselungsdienst darf mit den Chipkarten Kommandos MANAGE SECURITY ENVIRONMENT und PSO DECIPHER auf Chipkarten zugreifen.

(7) Das Subjekt S_AK darf mit den Chipkartenkommandos MANAGE SECURITY ENVIRONMENT, INTERNAL AUTHENTICATE, PSO COMPUTE DIGITAL SIGNATURE und GENERATE ASYMMETRIC KEY PAIR P1='81' auf den Schlüssel PrK.HCI.AUT zugreifen, wenn der Zugriff zu einem logischen Kanal einer SM-B gehört

(8) Nur der Chipkartendienst, der Signaturdienst, und der Verschlüsselungsdienst dürfen über einen logischen Kanal zu einer Chipkarte die Chipkartenkommandos MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE und MUTUAL AUTHENTICATE absetzen.

(9) Die Subjekte S_AK und S_Fachmodul, dürfen die Schließung des vom jeweiligen Subjekt angeforderten logischen Kanals anfordern. Der Chipkartendienst setzt den Sicherheitsstatus des logischen Kanals zurück.

(10) Der Chipkartendienst löscht das Kartenhandle, wenn die betreffende Chipkarte gezogen wird.

(11) Fachmodule und Clientsysteme können sich für die Ereignisse „CARD INSERTED“, „CARD REMOVED“, „CARD PIN VERIFY_STARTED“, „CARD PIN VERIFY_FINISHED“, „CARD PIN CHANGE_STARTED“, „CARD PIN CHANGE_FINISHED“, „CARD PIN ENABLE_STARTED“, „CARD PIN ENABLE_FINISHED“, „CARD PIN DISABLE_STARTED“ und „CARD PIN DISABLE_FINIS-

HED“ registrieren, um bei Eintritt der Ereignisse informiert zu werden.

(12) Das Clientssystem darf eine Benutzerauthentisierung anfordern.[221]

ST-Anwendungshinweis 31 Die Anforderung aus FDP_ACF.1.2/AK.KD(1) muss in Bezug auf das Caching der Daten präzisiert werden:

Alle zwischengespeicherten Daten, die über das Kartenhandle mit der Karte assoziiert werden, werden – sofern die Karte noch nicht entfernt wurde – nach 24 Stunden gelöscht und neu erzeugt. Für *eGK, HBAx* gilt zusätzlich, dass die existierenden Kartensitzungen gelöscht werden (vgl. auch TIP1-A_4558, bzw. TIP1-A_6031.)

FDP_ACF.1.3/AK.KD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[222]

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

(1) Kein Subjekt darf, wenn nicht ausdrücklich durch die Regeln in FDP_ACF.1.2/AK.KD erlaubt, auf private und symmetrische Schlüssel der Chipkarten mit den Chipkartenkommandos MANAGE CHANNEL, MANAGE SECURITY ENVIRONMENT, EXTERNAL AUTHENTICATE, GENERAL AUTHENTICATE, INTERNAL AUTHENTICATE oder MUTUAL AUTHENTICATE zugreifen.

(2) Kein Subjekt darf auf DF.KT einer gSMC-KT zugreifen.

(3) Der EVG verhindert schreibenden Zugriff auf Kartenobjekte der KVK.

(4) No further rule.[223]

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

FDP_ACC.1.1/AK.PIN The TSF shall enforce the VAD-SFP[224] on

subjects

(1) S_Chipkartendienst,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem,

[221] Assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
[222] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[223] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[224] Assignment: *access control SFP*

(4) PIN-Terminal,

(5) S_eHKT,

(6) S_eGK,

(7) S_HBA,

(8) S_HBAx,

(9) S_gSMC-KT,

(10) S_SMC-B,

objects:

(1) Authentisierungsverifikationsdaten (VAD) as plaintext,

(2) Authentisierungsverifikationsdaten (VAD) as ciphertext,

(3) SICCT-Kommando

operations:

(1) lokale PIN-Eingabe anfordern,

(2) lokale PIN-Eingabe durchführen,

(3) entfernte PIN-Eingabe anfordern,

(4) entfernte PIN-Eingabe durchführen,

(5) VAD an Chipkarten senden,

(6) VAD als Klartext verarbeiten,

(7) VAD als Geheimtext verarbeiten,

(8) VAD im Geheimtext ausgeben,

(9) SICCT-Kommandos übertragen

.[225]

FDP_ACF.1/AK.PIN

Security attribute based access control / PIN

FDP_ACF.1.1/AK.PIN

The TSF shall enforce the VAD-SFP[226] to objects based on the following: list of subjects, objects and security attributes:

subjects:

(1) S_Chipkartendienst,

(2) S_Signaturdienst,

(3) S_Fachmodul,

(4) S_AK,

(5) S_Benutzer_Clientsystem Authorisierungsstatus, with security attribute

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

[226] Assignment: *access control SFP*

(6) PIN-Terminal with security attribute Authorisierungsstatus,

(7) S_eHKT with security attribute Authorisierungsstatus,

(8) S_eGK mit dem Sicherheitsattribut CVC mit CHA, bzw. CHAT eGK,

(9) S_HBA mit dem Sicherheitsattribut CVC mit CHAT "PIN-Empfänger",

(10) S_HBAx mit Sicherheitsattribut „HBA" bzw. „HBA-VK",

(11) S_SMC-B mit dem Sicherheitsattribut CVC mit CHAT "PIN-Empfänger";

objects:

(1) Authentisierungsverifikationsdaten (VAD) as plaintext,

(2) Authentisierungsverifikationsdaten (VAD) as ciphertext,

(3) SICCT-Kommando

:[227]

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

(1) Das Subjekt S_AK, Fachmodule und das Clientsystem dürfen die lokale PIN-Eingabe und die entfernte PIN-Eingabe mit PIN-Referenz mit Ausnahme der Signatur-PIN und der Signatur-PUK für einen logischen Kanal einer Chipkarte beim Chipkartendienst anfordern.

(2) Das Subjekt „identifizierte Benutzer des Clientsystems" darf für die Signatur-PIN die lokale und entfernte PIN-Eingabe an seinem Arbeitsplatz für eine authentisierte Chipkarte zur PIN-Prüfung, zum PIN-Wechsel und zum Entsperren der PIN mit einer PUK anfordern.

(3) Das Subjekt Chipkartendienst darf die lokale PIN-Eingabe an authentisierten PIN-Terminal für jede identifizierte Chipkarte für alle PIN und PUK mit Ausnahme der Signatur-PIN und der Signatur-PUK durchführen.

(4) Das Subjekt Chipkartendienst darf die entfernte PIN-Eingabe an authentisierten PIN-Terminal mit einer authentisierten gSMC-KT als PIN-Sender für eine als PIN-Empfänger authentisierten HBA oder als PIN-Empfänger authentisierte SMC-B in einem authentisierten Chipkarten-Terminal für alle PIN und PUK mit Ausnahme der Signatur-PIN und der Signatur-PUK durchführen.

[227] Assignment: *ist of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

(5) Das Subjekt Signaturdienst darf die lokale PIN-Eingabe mit Signatur-PIN und Signatur-PUK am authentisierten PIN-Terminal für einen HBAx oder eine SMC-B für die PIN-Prüfung, den PIN-Wechsel oder PIN-Entsperren durchführen.

(6) Das Subjekt Signaturdienst darf die entfernte PIN-Eingabe mit der Signatur-PIN und der Signatur-PUK an authentisierten PIN-Terminals mit einer authentisierten gSMC-KT als PIN-Sender für eine als PIN-Empfänger authentisierten HBA oder als PIN- Empfänger authentisierte SMC-B in einem authentisierten Chipkarten-Terminal für die PIN-Prüfung, den PIN-Wechsel oder PIN-Entsperren durchführen.

(7) Die TSF steuert die PIN-Eingabe, so dass

a) wenn das PIN-Terminal und das Chipkarten-Terminal verschieden sind,

(i) ein gesicherter Kanal zwischen der gSMC-KT als PIN-Sender im PIN-Terminal und der Chipkarte als PIN-Empfänger im Chipkartenterminal vor der PIN-Eingabe aufgebaut wird,

(ii) das PIN-Terminal die eingegebene VAD im Klartext nur zum Verschlüsseln an die als PIN-Sender authentisiertegSMC-KT übergibt und nur die verschlüsselte VAD innerhalb des TLS-Kanals an den Konnektor übermittelt,

(iii) das Chipkartenterminal die verschlüsselte VAD nur für die PIN-Prüfung, das PIN-Entsperren oder den PIN- Wechsel dem als PIN-Empfänger authentisierten Heilberufsausweis oder der als PIN-Empfänger authentisierten SMC-B übergibt;

(b) wenn das PIN-Terminal und das Chipkarten-Terminal identisch sind, das PIN-Terminal die eingegebene VAD im Klartext nur für die PIN-Prüfung, PIN-Aktivierung, PIN-Deaktivierung, das PIN-Entsperren oder den PIN-Wechsel an die authentisierte eGK, den Heilberufsausweis und die SMC-B übergibt,

(c) die PIN-Eingabe am PIN-Terminal nur im gesicherten Mode erfolgt.[228]

FDP_ACF.1.3/AK.PIN The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[229].

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

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

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

(1) Kein Subjekt außer dem Chipkartendienst darf über den TLS-Kanal des EVG zu den eHealth-Kartenterminals SICCT-Kommandos mit dem Chipkartenkommando DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT, VERIFY, RESET RETRY COUNTER, DISABLE VERIFICATION REQUIREMENT, ENABLE VERIFICATION REQUIREMENT oder CHANGE REFERENCE DATA absetzen.

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

(3) no further rule[230].

6.3.3.4. Signaturdienst

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

FIA_SOS.2.1/AK.Jobnummer — The TSF shall provide a mechanism to generate **sechsstellige Jobnummern**[231] ~~**secrets**~~ that meet aus 3 zufälligen Großbuchstaben und 3 zufälligen Ziffern zu bestehen, wobei jedes Zeichen jeden Wert mit gleicher Wahrscheinlichkeit annimmt. Die TSF müssen sicherstellen, dass die letzten 1.000 vom EVG generierten Jobnummern einmalig sind[232].

FIA_SOS.2.2/AK.Jobnummer — The TSF shall be able to enforce the use of TSF generated **sechsstellige Jobnummern**[233] ~~**secrets**~~ for Übergabe der Jobnummern ans Clientsystem[234].

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

FDP_ACC.1.1/AK.Sgen — The TSF shall enforce the Signaturerstellung-SFP[235] on

subjects:

(1) S_AK,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem;

objects:

[230] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[231] Refinement
[232] Assignment: *a defined quality metric*
[233] Refinement
[234] Assignment: *list of TSF functions*
[235] Assignment: *access control SFP*

(1) Zu signierende Dokumente,

(2) Signaturstapel,

(3) Signierte Dokumente;

(4) Zu signierender Bitstring,

(5) Signierter Bitstring;

operations:

(1) Signatur erstellen,

(2) Signierte Dokumente erstellen,

(3) Signatur mit der Signaturkarte erstellen,

(4) Signaturvorgang abbrechen,

(5) Signierte Dokumente zurückgeben,

(6) Authentisierungsstatus der Signaturkarte zurücksetzen

.[236]

FDP_ACF.1/AK.Sgen

Security attribute based access control / Signaturerstellung

FDP_ACF.1.1/AK.Sgen

The TSF shall enforce the Signaturerstellung-SFP[237] to objects based on the following **list of subjects, objects and security attributes**[238]:

subjects:

(1) S_AK,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem with security attributes:

a) „Identität des Benutzers“,

b) „Authorisierungsstatus (HBA)“,

objects:

(1) Zu signierende Dokumente with security attributes:

a) Authorisierungsstatus: „nicht autorisiert“,

b) Authorisierungsstatus: „autorisiert“,

c) Signaturrichtlinie,

(2) Signaturstapel,

(3) Signaturschlüssel externer Signaturchipkarten,

(4) Signierte Dokumente with security attributes:

a) „ordnungsgemäß“

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

[237] Assignment: *access control SFP*

[238] Refinement

b) „ungültig“

(5) Zu signierender Bitstring,

(6) Signierter Bitstring,

(7) Authentisierungsschlüssel von HBAx oder SM-B.

:[239]

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

(1) Das Subjekt S_AK darf nur nicht autorisierte zu signierende Dokumente an das Subjekt Signaturdienst übergeben und die zu verwendende Signaturrichtlinie, den Signierenden, den Arbeitsplatz und die Signaturkarte identifizieren.

(2) Nur das Subjekt S_Signaturdienst steuert den Signaturprozess des identifizierten Arbeitsplatzes.

(3) Das Subjekt S_Signaturdienst darf nur dann die zu signierenden Dokumente signieren, wenn

(a) der Sicherheitsstatus der Signaturchipkarte die Erzeugung der digitalen Signatur erlaubt.

(4) Wenn die identifizierte Signaturrichtlinie die Erzeugung einer qualifizierte elektronische Signatur fordert, dann

(a) muss das Subjekt S_AK den Signierenden und den Arbeitsplatz identifizieren,

(b) muss die identifizierte Signaturrichtlinie für eine qualifizierte elektronische Signatur geeignet sein,

(c) muss das Subjekt S_Signaturdienst für die Einfachsignatur die lokale Eingabe der QES-PIN an HBAx oder die entfernte Eingabe der QES-PIN an HBA steuern und für die Stapelsignatur die lokale oder entfernte PIN-Eingabe für HBA steuern,

(d) darf das Subjekt S_Signaturdienst nur für durch den HBA „autorisierten Benutzer des Clientsystems“ zu signierenden Dokumente Signaturen mit der Signaturkarte erstellen, Signaturen ungültig signierter Dokumente sind zu löschen,

(e) das Subjekt S_Benutzer_Clientsystem darf den Signaturvorgang für die autorisierten zu signierenden Dokumente abbrechen,

(f) der S_Signaturdienst darf nur ordnungsgemäß signierte Dokumente an den S_AK zurückgeben,

[239] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

(g) das Subjekt S_Signaturdienst muss**, wenn die Komfortsignatur für die QSEE nicht aktiviert ist,** nach Abarbeitung des Stapels, bei Abbbruch des Signaturvorgangs durch das Subjekt S_Benutzer_Clientsystem und bei festgestellten ungültig signierten Dokumente den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA zurücksetzen.

(h) das Subjekt S_Signaturdienst muss, wenn die Komfortsignatur für die QSEE aktiviert ist, den Signatur-PIN-Authentisierungsstatus der Signaturkarte HBA zurücksetzen, wenn eins der folgenden Abbruchkriterien eintritt:

- ***SAK_COMFORT_SIGNATURE* wurde disabled,**[240]
- ***DeactivateComfortSignature* wurde aufgerufen,**[241]
- **HBA wurde gezogen,**[242]
- **Sicherheitszustand des HBA wurde zurückgesetzt oder der Kartenkontext wurde verlassen,**[243]

(i) das Subjekt S_Signaturdienst muss, wenn die Komfortsignatur für die QSEE aktiviert ist, den Signatur-PIN-Authentisierungsstatus der betreffenden Session der Signaturkarte HBA zurücksetzen, wenn eins der folgenden Abbruchkriterien eintritt:

- ***SAK_COMFORT_SIGNATURE_MAX* der Session wurde erreicht oder überschritten,**[244]
- ***SAK_COMFORT_SIGNATURE_TIMER* der Session ist abgelaufen. Läuft zu diesem Zeitpunkt ein Signaturvorgang in dieser Session, wird der Signaturvorgang beendet, bevor der Zustand zurückgesetzt wird. In diesem Fall muss das Subjekt S_AK die Annahme neuer Signaturvorgänge, die die Komfortsignatur für genau diese Session der Signaturkarte HBA nutzen wollen, ablehnen.**[245]

(5) Wenn die gültige Signaturrichtlinie die Erstellung einer qualifizierten elektronischen Signatur verlangt, darf das Subjekt S_Signaturdienst nur ordnungsgemäße qualifizierte elektronische Signaturen an den S_AK zurück geben.

[240] Refinement: *Gemäß Vorgaben aus A_19105*
[241] Refinement: *Gemäß Vorgaben aus A_19108*
[242] Refinement: *Gemäß Vorgaben aus TIP1-A_4671*
[243] Refinement: *Gemäß Vorgaben aus TIP1-A_4560*
[244] Refinement: *Gemäß Vorgaben aus A_19100-01*
[245] Refinement: *Gemäß Vorgaben aus A_18686-01*

(6) Das Subjekt S_AK darf dem S_Signaturdienst Binärstrings mit der maximalen Länge von 512 Bit nur zur Erstellung digitaler Signaturen mit Authentisierungsschlüsseln von HBAx oder SM-B übergeben und die von HBAx bzw. der SM-B signierte Binärstrings vom S_Signaturdienst empfangen.

FDP_ACF.1.3/AK.Sgen The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[246].

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

(1) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn der S_AK für die zu signierenden Dokumente eine Signaturrichtlinie zur Erstellung qualifizierter elektronische Signatur identifiziert, aber
   (a) der Signierende keine qualifizierte elektronische Signatur erzeugen kann oder
   (b) die Autorisierung des S_Benutzer_Clientsystem fehlschlägt.

(2) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für zu signierenden Dokumente verweigern, wenn für diese zu signierenden Dokumente und den Signierenden die identifizierte Signaturrichtlinie ungültig ist.

(3) Das Subjekt S_Signaturdienst muss die Erstellung der Signatur für den Signaturstapel verweigern und alle für zu signierende Dokumente des Signaturstapels bereits erzeugten Signaturen löschen, wenn die Überprüfung der Signatur wenigstens einer signierten Datei des Signaturstapels fehlschlägt.

(4) Außer dem S_Signaturdienst darf kein Subjekt auf
   (a) das Verzeichnis DF.QES des HBA,
   (b) den Schlüssel PrK.HCI.OSIG der SMC-B,
   (c) keine weiteren Einschränkungen[247]

   zugreifen.

(5) Das Subjekt S_AK muss die Erstellung der Signatur für SAML2-Assertions verweigern, wenn die Aufforderung zur Signatur nicht von einem Fachmodul an den S_AK gerichtet wurde[248].

[246] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[247] Assignment: *weitere Signaturschlüssel externer Signaturchipkarten*
[248] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*

FDP_ACC.1/AK.SigPr
Subset access control / Signature verification

FDP_ACC.1.1/AK.SigPr

The TSF shall enforce the Signature verification-SFP[249] on subjects:

(1) S_AK,

(2) S_Signaturdienst,

(3) S_Benutzer_Clientsystem;

objects:

(1) Signierte Dokumente,

(2) Signaturprüfungsergebnis;

operations:

(1) Signatur prüfen,

(2) Festlegen des angegebenen Zeitpunkts

.[250]

FDP_ACF.1/AK.SigPr
Security attribute based access control / Signature verification

FDP_ACF.1.1/AK.SigPr

The TSF shall enforce the Signature verification-SFP[251] to objects based on the following **list of subjects, objects and security attributes**[252]:

subjects

(1) S_AK

(2) S_Signaturdienst

(3) S_Benutzer_Clientsystem;

objects:

(1) Signierte Dokumente with the security attributes

a) Signaturrichtlinie

b) Angegebener Zeitpunkt,

(2) Signaturprüfungsergebnis

.[253]

FDP_ACF.1.2/AK.SigPr

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[249] Assignment: *access control SFP*

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

[251] Assignment: *access control SFP*

[252] Refinement

[253] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

(1) Das Subjekt S_AK darf signierte Dokumente an das Subjekt S_Signaturdienst zur Signaturprüfung übergeben und die Signaturrichtlinie identifizieren.

(2) Der Signaturdienst darf das Ergebnis der Signaturprüfung an das Subjekt S_AK zurückgeben.

:[254]

FDP_ACF.1.3/AK.SigPr — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[255].

FDP_ACF.1.4/AK.SigPr — The TSF shall explicitly deny access of subjects to objects based on the following additional rules: no further rule[256].

FDP_DAU.2/AK.QES

Data Authentication with Identity of Guarantor / Qualifizierte elektronische Signatur

FDP_DAU.2.1/AK.QES — The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of data to be signed **durch qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der qualifizierten Signaturerstellungseinheit (QSEE) zur Erzeugung der digitalen Signatur. Es sind die Dokumentenformate zu signierender Daten**

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

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

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

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

und die Formate signierter Daten

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

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

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

mit den Signaturvarianten

(1) **enveloped signature,**

(2) **enveloping signature,**

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

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

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

(3) detached signature[257]

zu unterstützen.

ST-Anwendungshinweis 32

Anwendungshinweis 160 des Schutzprofils eröffnet dem Hersteller die Möglichkeit, auch *detached signatures* zu verwenden, falls ein Fachmodul dies erfordert. Das Fachmodul NFDM benötigt eine solche Signatur. Die vom TOE angesteuerte Karte erstellt die Signatur, der TOE selbst bereitet die Daten für den Signaturvorgang auf. Die Möglichkeit der detached signature gilt ausschließlich im Kontext von XML-Signaturen.

ST-Anwendungshinweis 33

Die Konnektorspezifikation schränkt die Kombinationsmöglichkeiten von Dokumentformaten, Signaturformaten und Signaturvarianten in TAB_KON_778 deutlich ein. Der TOE folgt der Konnektorspezifikation weitgehend. Der genaue Funktionsumfang des TOEs ist in ASE_TSS unter der Überschrift „Signaturrichtlinien“ in Unterabschnitt 7.2.7 beschrieben.

FDP_DAU.2.2/AK.QES

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

Dies sind im einzelnen:

- **(1) ob die signierten Daten unverändert sind, d. h. das Ergebnis der Korrektheitsprüfung der digitalen Signatur über die signierten Daten,**
- **(2) der der Signatur zuzuordnende Signaturschlüssel-Inhaber,**
- **(3) die Inhalte des Zertifikates, auf dem die Signatur beruht,**
- **(4) das Ergebnis der Nachprüfung der Zertifikate nach dem Kettenmodell, d. h. die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,**
  - **a. der angenommene Signaturerstellungszeitpunkt, wobei gegen folgende Zeitpunkte zu prüfen ist, sofern die Voraussetzungen durch die zu prüfenden Daten erfüllt sind:**
    - **i. vom Benutzer definierter Zeitpunkt, sonst**
    - **ii. in der Signatur eingebetteter Zeitpunkt, sonst**

[257] Refinement: *ST-Anwendungshinweis 32*

iii. *none*[258]**,**

iv. bzw. wenn diese nicht vorliegen der Jetzt-Zeitpunkt;

b. das Vorhandensein des Zertifikats des VDA, der das Signaturzertifikat ausgestellt hat, in der BNetzA-VL,

c. die Korrektheit der digitalen Signatur des Zertifikats mit Ausnahme des Wurzelzertifikats,

d. die Anforderung von OCSP-Anfragen und die Auswertung von OSCP-Antworten, ob das nachgeprüfte qualifizierte Signaturzertifikat im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war.

(5) Für jedes Ergebnis der Korrektheitsprüfung einer digitalen Signatur ist anzugeben, ob

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

b. die für Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum angegeben Signaturerstellungszeitpunkt geeignet waren, wenn dies nicht der Fall ist, liegt keine qualifizierte elektronische Signatur vor;

c. die für die Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum Signaturprüfzeitpunkt geeignet sind; wenn dies nicht der Fall ist, ist eine Information zum verminderten Beweiswert der qualifizierte elektronischen Signatur zurückzugeben.

(6) keine weiteren Nachweise[259]**.**

FDP_DAU.2/AK.Sig

Data Authentication with Identity of Guarantor / NonQES

FDP_DAU.2.1/AK.Sig

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of zu signierenden Daten[260] **durch nicht-qualifizierte elektronische Signatur gemäß gültiger Signaturrichtlinie mit Hilfe der Chipkarten. Es sind die Dokumentenformate zu signierender Daten**

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

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

[259] Assignment: *andere Form von Nachweisen*

[260] Assignment: *list of objects or information types*

(2) TIFF-Dateien [TIFF],

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

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

(5) Binärdokument,

und die Formate signierter Daten

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

(2) CAdES [CAdES; CAdES-BL] für Text, TIFF, Adobe Portable Document Format (PDF/A) und XML Dokumente sowie Binärdokumente,

mit den Signaturverfahren

(1) enveloped signature,

(2) enveloping signature,

(3) detached signature

zu unterstützen.[261]

ST-Anwendungshinweis 34

Die Erläuterungen aus ST-Anwendungshinweis 33 gelten ebenfalls für dieses SFR.

FDP_DAU.2.2/AK.Sig

The TSF shall provide S_Benutzern with the ability to verify evidence of the validity of the indicated information ~~**and the identity of the user that generated the evidence**~~ **durch nicht-qualifizierte elektronische Signatur in den in FDP_DAU.2.1/AK.Sig genannten Formaten sowie PKCS#1 RSASSA-PSS und RSASSA-PKCS1-v.5 [RFC 8017] gemäß gültiger Signaturrichtlinie bereitstellen. Dies sind im einzelnen:**

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

(2) der Signatur zuzuordnende Signaturschlüssel-Inhaber,

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

(4) das Ergebnis der Nachprüfung von Zertifikaten in der Zertifikatskette,

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

(6) keine weiteren Nachweise[262]**.**

[261] Refinement

[262] Assignment: *andere Form von Nachweisen*

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

FDP_DAU.2.1/AK.Cert — The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of Signaturen[263].

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

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

(2) die zugehörigen Attribut-Zertifikate,

(3) der der Signatur zuzuordnende Signaturschlüssel-Inhaber,

(4) die Gültigkeit der Zertifikate zum angegebenen Zeitpunkt,

(5) das Ergebnis der Korrektheitsprüfung der Signatur,

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

(7) ob die signierten Daten unverändert sind,

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

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

(10) keine weiteren Nachweise.[264]

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

FDP_ITC.2.1/AK.Sig — The TSF shall enforce the Signaturerstellung-SFP und Signaturprüfung-SFP[265] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

[263] Assignment: *list of objects or information types*
[264] Assignment: *andere Form von Nachweisen*
[265] Assignment: *access control SFP(s) and/or information flow control SFP(s)*

FDP_ITC.2.5/AK.Sig

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

(1) Die TSF importiert zu signierende Daten mit dem Sicherheitsattribut „Signaturrichtlinie“ nur nach erfolgreicher Prüfung der Zulässigkeit der Signaturrichtlinie.

(2) Die TSF importiert zu prüfende signierte Daten mit dem Sicherheitsattribut „Signaturrichtlinie“ nur nach erfolgreicher Prüfung der Zulässigkeit der Signaturrichtlinie.

(3) Eine Signaturrichtlinie für qualifizierte elektronische Signaturen ist zulässig, wenn

a) für die Erzeugung einer qualifizierten elektronischen Signatur eine Benutzersteuerung festgelegt ist,

b) die Signaturprüfung mit anzeigbarem erzeugtem Prüfprotokoll erfolgt,

c) die Signaturrichtlinie auf die zu signierenden Daten durch den EVG anwendbar ist.

(4) Die TSF weist importierten zu signierenden Daten das Sicherheitsattribut „nicht autorisiert“ zu

.[266]

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

FMT_MSA.3.1/AK.Sig

The TSF shall enforce the Signaturerstellung-SFP und die Signaturprüfung-SFP to provide *restrictive* default values for security attributes zulässige Signaturrichtlinie **and configuration values *SAK_COMFORT_SIGNATURE*, *SAK_COMFORT_SIGNATURE_MAX* and *SAK_COMFORT_SIGNATURE_TIMER***[267] that are used to enforce the SFP.

FMT_MSA.3.2/AK.Sig

The TSF shall allow the Administrator[268] to specify alternative initial values to override the default values when an object or information is created.

FDP_SDI.2/AK
Stored data integrity monitoring and action

FDP_SDI.2.1/AK

The TSF shall monitor ~~**user data**~~ **zu signierende Daten** stored in containers controlled by the TSF for Veränderung on all objects, based on the following attributes: SHA-256 hash of the data[269].

[266] Assignment: *additional importation control rules*
[267] Refinement: *Gemäß Vorgaben aus A_18686-01, Standardablauf in A_19106-02 und Standardablauf in A_19104-04*
[268] Assignment: *the authorised identified roles*
[269] Assignment: *user data attributes*

FDP_SDI.2.2/AK

Upon detection of a data integrity error, the TSF shall

(1) Die Erstellung der digitalen Signatur für die zu signierenden Daten verweigern und den Benutzer des Clientsystems über den Datenintegritätsfehler informieren,

(2) keine weiteren Aktionen ausführen.[270]

FMT_MSA.1/AK.User

Management of security attributes / Clientsystem-Benutzer

FMT_MSA.1.1/AK.User

The TSF shall enforce the Signaturerstellung-SFP und die Signaturprüfung-SFP[271] to restrict the ability to

(1) *Modify*[272] the security attribute**s** Autorisierungsstatus zu signierender Daten,[273]

(2) *Select*[274] the security attributes gültige Signaturrichtlinie für zu signierende Daten,[275]

(3) *Modify*[276] the security attributes angegebener Zeitpunkt signierter Daten für die Signaturprüfung[277] [278]

to S_Benutzer_Clientsystem[279].

ST-Anwendungshinweis 35

Da der Begriff Signaturrichtlinie im PP abstrakt alle Input-Parameter einer Signaturerstellung oder -prüfung umfasst, wird FMT_MSA.1.1/AK.User(2) dahingehend interpretiert, dass die Auswahl von Parametern durch den Benutzer des Clientsystems durchgeführt wird, vgl. auch die Beschreibung zu SF.SignatureService in Unterabschnitt 7.2.7.

FTP_ITC.1/AK.QSEE

Inter-TSF trusted channel / QSEE

FTP_ITC.1.1/AK.QSEE

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **der qualifizierten Signaturerstellungseinheit**[280] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification **and**[281] ~~**or**~~ disclosure.

[270] Assignment: *weitere auszuführende Aktion*
[271] Assignment: *access control SFP(s), information flow control SFP(s)*
[272] Selection: *change_default, query, modify, delete, [assignment: other operations]*
[273] Assignment: *list of security attributes*
[274] Selection: *change_default, query, modify, delete, [assignment: other operations]*
[275] Assignment: *list of security attributes*
[276] Selection: *change_default, query, modify, delete, [assignment: other operations]*
[277] Assignment: *list of security attributes*
[278] Refinement
[279] Assignment: *the authorised identified roles*
[280] Refinement
[281] Refinement

FTP_ITC.1.2/AK.QSEE	The TSF shall permit *the TSF*[282] to initiate communication via the trusted channel.
FTP_ITC.1.3/AK.QSEE	The TSF shall initiate communication via the trusted channel for Senden der zu signierende Daten an die qualifizierte Signaturerstellungseinheit[283].
ST-Anwendungshinweis 36	FTP_ITC.1.3/AK.QSEE bezieht sich auf die Stapel- und Komfortsignatur. Für eine Einfachsignatur ist die Nutzung von Secure Messaging nicht erforderlich (vgl. TIP1-A_4670 [gemSpec_Kon] und A_19258 [gemSpec_Kon].

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

FTA_TAB.1.1/AK.Jobnummer	Before **entfernter Eingabe von PIN und PUK an eHealth- Kartenterminals**[284] ~~**establishing a user session**~~, the TSF shall display **die vom Clientsystem übergebene und vom EVG geprüfte Jobnummer an eHealth-Kartenterminal**[285] ~~**an advisory warning message**~~ regarding **nichtbeabsichtigten**[286] ~~**unauthorised**~~ use of the TOE.

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

FTA_TAB.1.1/AK.SP	~~**Before establishing a user session**~~ **Bei Feststellung ungültig erzeugter Signaturen,**[287] the TSF shall display an advisorywarning message regarding unauthorised use of the TOE **to S_Benutzer_Clientsystem via the standard interface.**
ST-Anwendungshinweis 37	Die Kommunikation zwischen TOE und S_Benutzer_Clientsystem erfolgt über SOAP-Nachrichten und deren Interpretation durch die Benutzerschnittstelle des Clientsystemems. Der TOE hat selbst keine visuelle Benutzerschnittstelle zum Subjekt S_Benutzer_Clientsystem, über die die Warnung ausgegeben werden kann. Folglich wird das Refinement so interpretiert, dass die geforderte *advisory warning message* über die Antwort zum SOAP-Request übermittelt wird.

[282] Selection: *the TSF, another trusted IT product*
[283] Assignment: *list of functions for which a trusted channel is required*
[284] Refinement
[285] Refinement
[286] Refinement
[287] Refinement

6.3.3.5. Software-Update

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

FDP_ACC.1.1/AK.Update

The TSF shall enforce the Update-SFP[288] on

subjects:

(1) S_Administrator,

(2) S_AK,

(3) S_NK,

objects:

(1) Update-Pakete,

(2) O_Zertifikat_gSMC-K[289]

operations:

(1) Importieren

(2) Verwenden,

Operation	Beschreibung	Anmerkung
Importieren	Einlesen von bereitgestellten Update-Paketen und Aktualisieren der Komponenten des EVG	Der Download kann automatisch erfolgen
Verwenden	Die Update-Pakete werden zum Update der TSF-Daten, zum Update des EVG zu einem neuen EVG oder zum Update anderer externer Komponenten (eHealth-Kartenterminal) verwendet.	Das Installieren (Verwenden) des Updates kann automatisch erfolgen.

[290]

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

FDP_ACF.1.1/AK.Update

The TSF shall enforce the Update-SFP[291] to objects based on the following:

subjects:

[288] Assignment: *access control SFP*
[289] Refinement: *Gemäß Vorgaben aus A_21749-03*
[290] Assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*
[291] Assignment: *access control SFP*

(1) S_Administrator,

(2) S_AK,

(3) S_NK,

objects:

(1) Update-Pakete with security attributes,

a) Signatur

b) Zulässige Software-Versionen

(2) O_Zertifikat_gSMC-K mit Sicherheitsattributen

a) ICCSN,

b) öffentlicher Schlüssel,

c) Ablaufdatum

d) Signatur[292]

:[293]

FDP_ACF.1.2/AK.Update

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Das Subjekt S_AK oder S_NK darf nur Update-Pakete importieren, deren Signatur erfolgreich geprüft wurde.

(2) Die Subjekte S_Administrator, S_AK und S_NK dürfen nur Update-Pakete verwenden, die einer Firmwaregruppe angehören, die gleich oder höher der gegenwärtig installierten Firmwaregruppe ist.

(3) Die Subjekte S_AK oder S_NK dürfen O_Zertifikat_gSMC-K nur importieren, wenn die Prüfungen aus TUC_KON_410 erfolgreich waren:

a) ICCSN des neuen und alten Zertifikats sind gleich,

b) Ablaufdatum des neuen Zertifikats liegt nach Ablaufdatum des alten Zertifikats,

c) Kryptografische Prüfung, dass öffentlicher Schlüssel im neuen Zertifikat zum privaten Schlüssel auf der gSMC-K passt,

d) Für C.NK.VPN, C.AK.AUT, C.SAK.AUT: Zertifikatsprüfung nach TUC_KON_037, bei C.NK.VPN mit Parameter *validationMode = OCSP*

e) Für C.SAK.AUTD_CVC, C.CA_SAK.CS:

[292] Refinement: *Gemäß Vorgaben aus A_21749-03*

[293] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

i.) Prüfung der Signatur von C.SAK.AUTD_CVC gegen C.CA_SAK.CS

ii.) Ermittlung des passenden CVC-Root-Zertifikats im Truststore und Prüfung von C.CA_SAK.CS dagegen

f) Prüfung, dass C.SAK.AUTD_CVC dem Profil CHAT.51 entspricht.[294]

:[295]

FDP_ACF.1.3/AK.Update — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[296].

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

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

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

(3) Wenn ein Update-Paket mit *FWPriority=Kritisch* vorhanden ist, dessen Deadline abgelaufen ist, so darf die TSF keine Kommunikation mit der TI Plattform herstellen und muss bestehende Verbindungen zur TI Plattform abbauen.[297]

(4) Der TOE darf ein erneuertes C.AK.AUT nicht automatisch verwenden, wenn S_Administrator es nicht explizit zur Verwendung ausgewählt hat.[298]

ST-Anwendungshinweis 38 — Der TOE unterstützt die automatische Anwendung von Update-Paketen gemäß A_18390 und A_18391.

ST-Anwendungshinweis 39 — TIP1-A_6025 wird umgesetzt durch Unterpunkt FDP_ACF.1.1/AK.Update(3).

[294] Refinement: *Gemäß Vorgaben aus A_21749-03*
[295] Assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
[296] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[297] Refinement: *Gemäß Vorgaben aus TIP1-A_6025*
[298] Refinement: *Gemäß Vorgaben aus A_21759*

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

FDP_UIT.1.1/AK.Update — The TSF shall enforce the Update-SFP[299] to *receive*[300] user data ~~**in a manner**~~ protected from *modification, deletion, insertion*[301] errors.

FDP_UIT.1.2/AK.Update — The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion*[302] has occurred.

6.3.3.6. Verschlüsselungsdienst

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

FDP_ACC.1.1/AK.Enc — The TSF shall enforce the Verschlüsselung-SFP[303] on

subjects:

(1) S_AK

(2) S_Verschlüsselungsdienst;

objects:

(1) Zu verschlüsselnde Daten,

(2) Verschlüsselte Daten,

(3) Zu entschlüsselnde Daten,

(4) Entschlüsselte Daten;

operations:

(1) Verschlüsseln,

(2) Entschlüsseln,

(3) Festlegen der vorgesehenen Empfänger[304].

FDP_ACF.1/AK.Enc
Security attribute based access control / Verschlüsselung

FDP_ACF.1.1/AK.Enc — The TSF shall enforce the Verschlüsselung-SFP[305] to objects based on the following:

subjects:

(1) S_AK,

(2) S_Verschlüsselungsdienst;

[299] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[300] Selection: *transmit, receive*
[301] Selection: *modification, deletion, insertion, replay*
[302] Selection: *modification, deletion, insertion, replay*
[303] Assignment: *access control SFP*
[304] Assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*
[305] Assignment: *access control SFP*

objects:

(1) Zu verschlüsselnde Daten with security attributes:
   a) Verschlüsselungsrichtlinie,
   b) Vorgeschlagene Empfänger,
   c) Objekt-ID,

(2) verschlüsselte Daten with security attributes:
   a) Verschlüsselungsrichtlinie,
   b) Vorgeschlagene Empfänger,
   c) Ordnungsgemäss verschlüsselt,

(3) Zu entschlüsselnde Daten with security attributes:
   a) Verschlüsselungsrichtlinie,
   b) Vorgeschlagene Empfänger

(4) Entschlüsselte Daten

:[306]

FDP_ACF.1.2/AK.Enc

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Das Subjekt S_AK muss zu verschlüsselnde Daten an das Subjekt S_Verschlüsselungsdienst mit der Objekt-ID, der Identität der Verschlüsselungsrichtlinie und der Identität der vorgeschlagenen Empfängern übergeben.

Der Verschlüsselungsdienst darf Requests zur Verschlüsselung nur akzeptieren, wenn sie konform zur gematik Spezifikation sind, vgl. [gemSpec_Kon, TAB_KON_739, TUC_KON_070].[307]

(2) Das Subjekt S_Verschlüsselungsdienst darf nur ordnungsgemäß verschlüsselte Daten oder Statusmeldungen an das Subjekt S_AK zurückgeben.

(3) Das Subjekt S_Verschlüsselungsdienst darf nur dann die zu verschlüsselnden Daten für die identifizierten vorgeschlagenen Empfänger automatisch verschlüsseln, wenn
   1. die identifizierte Verschlüsselungsrichtlinie für die übergebenen zu verschlüsselnden Daten zulässig ist,
   2. die identifizierte Verschlüsselungsrichtlinie die automatische Verschlüsselung erlaubt,
   3. die Verschlüsselungszertifikate der vorgeschlagenen Empfänger gültig sind.

[306] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*
[307] Refinement: *vgl. ST-Anwendungshinweis 40*

(4) Das Subjekt S_AK darf zu entschlüsselnde Daten an das Subjekt S_Verschlüsselungsdienst nur mit Identität eines vorgesehenen Empfängers, dessen Chipkarte für die Entschlüsselung benutzt werden soll, und der Identität der zum Entschlüsseln zu verwendenden Verschlüsselungsrichtlinie übergeben.

Der Verschlüsselungsdienst darf Requests zur Entschlüsselung nur akzeptieren, wenn sie konform zur Gematik Spezifikation sind, vgl. [gemSpec_Kon, TAB_KON_140 TUC_KON_071].[308]

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

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

FDP_ACF.1.3/AK.Enc — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[309].

FDP_ACF.1.4/AK.Enc — The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[310].

ST-Anwendungshinweis 40 — Der Begriff „Verschlüsselungsrichtlinie“ muss interpretiert werden. Im PP wird der Begriff im Glossar definiert. Er umfasst im wesentlichen das Verschlüsselungsformat (CMS oder XMLSec), den Herausgeber der Verschlüsselungsrichtlinie und – im Fall von XMLSec – das XML-Schema und die Information, ob der Schlüssel im Dokument steht. Die gematik Spezifikation verwendet den Begriff der Verschlüsselungsrichtlinie nicht, definiert aber dei Aufrufparameter für die Operationen *EncryptDocument* und *DecryptDocument*. Die gematik Spezifikation ist damit deutlich präziser als das Schutzprofil. Daher gilt für dieses Security Target die folgende Interpretation.

Die Forderung nach einer *zulässigen Verschlüsselungsrichtlinie* wird so interpretiert, dass die gegebene Kombination von Aufrufparametern im Rahmen des spezifizierten Regelwerkes als gültig bewertet wird. Für den TOE werden die Vorgaben der Konnektor Spezifikation als Regelwerk angenommen. Die Eingangsdaten der TUCs

[308] Refinement: *vgl. ST-Anwendungshinweis 40*
[309] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[310] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*

TUC_KON_070 und TUC_KON_071 liefern sehr präzise Vorgaben für die Parameter. Die Interpretation gilt nicht nur hier, sondern auch für alle weiteren Vorkommen von „Verschlüsselungsrichtlinie“ in diesem Security Target.

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

FDP_ITC.2/AK.Enc

Import of user data with security attributes / Verschlüsselungsdienst

FDP_ITC.2.1/AK.Enc — The TSF shall enforce the Verschüsselungs-SFP[311] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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

(1) Die TSF importiert zu verschlüsselnde Daten mit dem Sicherheitsattribut „Verschlüsselungsrichtlinie“ nur für die identifizierten Fachanwendungen bzw. Anwendungsfälle und implementierten Verschlüsselungsrichtlinien.

(2) Die TSF importiert Verschlüsselungszertifikate und zu verschlüsselnde Daten mit dem Sicherheitsattribut „vorgeschlagene Empfänger“ nur nach erfolgreicher Prüfung der Gültigkeit der Verschlüsselungszertifikate der vorgesehenen Empfänger.

(3) Die TSF importiert TI-fremde X.509 CA-Zertifikate durch den Administrator über die Management-Schnittstelle

.[312]

ST-Anwendungshinweis 41 — Die Anforderung FDP_ITC.2.5/AK.Enc(2) wird so interpretiert, dass die Prüfung der Gültigkeit der Verschlüsselungszertifikate vor deren Verwendung zur Verschlüsselung eines Dokuments erfolgen muss.

[311] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[312] Assignment: *additional importation control rules*

FDP_ETC.2/AK.Enc

Export of user data with security attributes / Verschlüsselungsdienst

FDP_ETC.2.1/AK.Enc	The TSF shall enforce the Verschüsselungs-SFP[313] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2/AK.Enc	The TSF shall export the user data with the user data's associated security attributes
FDP_ETC.2.3/AK.Enc	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/AK.Enc	The TSF shall enforce the following rules when user data is exported from the TOE: (1) Die TSF exportieren verschlüsselte Daten mit der Identität des vorgesehenen Empfängers bzw. den Identitäten der vorgesehenen Empfänger und der Identität der verwendeten Verschlüsselungsrichtlinie. (2) Die TSF exportieren entschlüsselte Daten mit der Identität des vorgesehenen Empfängers, dessen Chipkarte zum Entschlüsseln benutzt wurde. (3) No further rules[314].
ST-Anwendungshinweis 42	Die Anforderung FDP_ETC.2.4/AK.Enc(2) wird so interpretiert, dass die entschlüsselten Daten ausschließlich an den vorgesehenen Empfänger ausgeliefert werden. Die Identität des Empfängers manifestiert sich nicht in der Datenstruktur der Ausgabe der Operation. Die Spezifikation der gematik gibt ein solches Identifizierungsmerkmal nicht her[315]. In der vorliegenden Implementierung werden die entschlüsselten Daten in genau der HTTP-Response übertragen, die zu dem Request gehört, über den die zu entschlüsselnden Daten in den TOE importiert wurden. Damit ist die eindeutige Zuordnung des Empfängers gewährleistet.

6.3.3.7. TLS-Kanäle

FDP_ACC.1/AK.TLS

Subset access control / TLS-Kanäle

FDP_ACC.1.1/AK.TLS	The TSF shall enforce the AK-TLS-SFP[316] on subjects:

[313] Assignment: *access control SFP(s) and/or information flow control SFP(s)*

[314] Assignment: *additional exportation control rules*

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

[316] Assignment: *access control SFP*

(1) S_AK,

(2) S_NK

(3) S_Clientsystem,

(4) S_Fachmodul,

(5) S_Fachdienst,

(6) S_Verzeichnisdienst (VZD)

(7) S_KSR

(8) S_TSL_Dienst

(9) S_Administrator

objects:

(1) Zu sendende Daten

(2) Empfangene Daten

(3) TLS-Kanal

operations:

(1) Aufbau des TLS-Kanals,

(2) Abbau des TLS-Kanals

(3) Unterbrechen und Wiederaufnahme der TLS-Verbindung mit Session ID (nur VSDM),

(4) Anfordern zur Wiederaufnahme einer TLS- Verbindung mit Session ID (nur VSDM),

(5) senden

(6) empfangen

.[317]

ST-Anwendungshinweis 43 Für das Fachmodul ePA setzt der TOE das Subjekt S_TLS_Dienst um. Fachmodule erhalten nach Anforderung einer TLS-Verbindung einen Identifier. Die Kenntnis dieses Identifiers ist notwendig, um die TLS-Verbindung nutzen zu können. Innerhalb des TOEs wird S_TLS_Dienst nicht verwendet. Die Module des TOE können TLS-Verbindungen über die Methoden des JSSE-Frameworks öffnen und nutzen.

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

FDP_ACF.1.1/AK.TLS The TSF shall enforce the AK-TLS-SFP[318] to objects based on the following:

subjects:

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

[318] Assignment: *access control SFP*

(1) S_AK,

(2) S_NK,

(3) S_Clientsystem,

(4) S_Fachmodul with or without the security attribute “VSDM (VSDM-Fachmodul)”,

(5) S_Fachdienst with or without the security attribute “Intermediär VSDM (Intermediär VSDM)”,

(6) S_Verzeichnisdienst (VZD),

(7) S_KSR,

(8) S_TSL_Dienst

objects:

(1) Zu sendende Daten,

(2) Empfangene Daten,

(3) TLS-Kanal with the security attribute „Anfordernder TLS-Client“

:[319]

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

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

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

(3) Nur der anfordernde TLS-Client darf unter Angabe des TLS-ConnectionIdentifiers zu sendende Daten an das S_AK zur Übertragung im TLS-Kanal übergeben.

(4) Das S_AK darf über den TLS-Kanal empfangene Daten nur an den anfordernden TLS-Client übergeben.

(5) Nur der anfordernde TLS-Client darf den S_AK zum Abbau des TLS-Kanals auffordern.

(6) Wenn MGM_LU_ONLINE = Enabled darf das S_AK eine SessionID des Intermediär VSDM empfangen und dem TLSConnectionIdentifier zuordnen. Das S_AK darf auf Anforderung des VSDM-Fachmoduls die unterbrochene Sitzung

[319] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

des TLS-Kanals zum Intermediär VSDM mit der SessionID wiederaufnehmen, wenn das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial nicht älter als 24 Stunden ist.

(7) Wenn MGM_LU_ONLINE = Enabled und MGM_LOGICAL_SEPARATION = Disabled dann baut das S_AK mit dem LDAP-Proxy auf Anforderung des Clientsystems oder eines Fachmoduls (Search Request) eine LDAPv3 Verbindung zum VZD auf.

(8) Wenn MGM_LU_ONLINE = Enabled und MGM_LOGICAL_SEPARATION = Disabled dann baut das S_AK mit dem LDAP-Proxy auf Anforderung des Clientsystems oder eines Fachmoduls (Unbind Request) eine LDAPv3 Verbindung zum VZD ab.

(9) Wenn ANCL_TLS_MANDATORY = Enabled so nimmt S_AK die Aufforderung des Clientsystems zum Aufbau eines TLS-Kanals entgegen und darf nur über diesen Kanal mit Clientsystemen kommunizieren. ~~**Ausgenommen ist die Kommunikation mit Dienstverzeichnisdienst bei gesetzter Variable ANCL_DVD_OPEN = Enabled.**~~[320]

(10) Die Subjekte S_NK und S_AK dürfen für den Download von Firmware-Update-Paketen einen TLS-Kanal zum S_KSR aufbauen.

(11) Das S_AK baut für den Download der BNetzA-VL und deren Hash-Wert sowie der TSL und deren Hash-Wert einen TLS-Kanal zum TSL-Dienst auf.

(12) Wenn *ANCL_CAUT_MANDATORY = Enabled*, so nimmt S_AK die Aufforderung des Clientsystems zum Aufbau eines TLS-Kanals an der HTTP/SOAP-Schnittstelle LS.LAN.HTTP nur dann entgegen, wenn sich das Clientsystem mit einem der Authentisierungsverfahren gemäß *ANCL_CAUT_MODE* und FIA_UAU.5/AK(5) authentisiert hat.

(13) Wenn *ANCL_CAUT_LDAP = Enabled*, so nimmt S_AK die Aufforderung des Clientsystems zum Aufbau eines TLS-Kanals an der LDAP-Schnittstelle LS.LAN.LDAP nur dann entgegen, wenn sich das Clientsystem mit einem X.509-Zertifikat gemäß FIA_UAU.5/AK(5) authentisiert hat.[321]

FDP_ACF.1.3/AK.TLS The TSF shall explicitly authorise access of subjects to objects based

[320] Deletion: *Vgl. ST-Anwendungshinweis 44*

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

on the following additional rules: none[322].

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

(1) Wenn MGM_LU_ONLINE = “Disabled“, DARF der Basisdienst TLS-Dienst nach dem Bootup NICHT TLS-Kanäle zur Verfügung stellen.

(2) Der Intermediär VSDM kann die Nutzung der SessionID zur Wiederaufnahme der TLS-Verbindung ablehnen und den Aufbau einer TLS-Verbindung verlangen.

(3) Wenn MGM_LU_ONLINE = “Disabled“ oder MGM_LOGICAL_SEPARATION=Enabled, DARF die Verzeichnisverwaltung NICHT TLS-Kanäle zum VZD zur Verfügung stellen.

(4) The TSF shall perform den Kanal zum VZD 15 Minuten nach der letzten vom VZD empfangenen oder von der Verzeichnisverwaltung des EVG gesendeten Daten abbauen.

(5) no further rules[323]

ST-Anwendungshinweis 44 — Die Funktionalität zur unverschlüsselten Kommunikation mit dem Dienstverzeichnisdienst bei ansonsten verpflichtender TLS-Verbindung wurde in Absprache mit der Prüfstelle entfernt.

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

FMT_MSA.1.1/AK.TLS — The TSF shall enforce the AK-TLS-SFP to restrict the ability to change_default, query, modify, delete, none[324] the security attributes Authentisierungsmechanismus[325] to S_Administrator.

Änderungen der Konfiguration müssen unmittelbar durchgesetzt werden.

ST-Anwendungshinweis 45 — Die Konnektor-Spezifikation definiert in TAB_KON_852 zu TIP1-A_5009 die Zugriffsregeln, die sich aus den Kombinationen der Konfigurationswerte ergeben. Das Assignment „Authentisierungsmechanismus“ schließt diese Konfigurationswerte ein.

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

FMT_MSA.3.1/AK.TLS — The TSF shall enforce the AK-TLS-SFP to provide *unmodifiable*[326] default values for security attributes that are used to enforce the SFP.

[322] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[323] Assignment: *additional rules, based on security attributes, that explicitly deny access of subjects to objects*
[324] Assignment: *other operations*
[325] Assignment: ***Authentisierungsmechanismus**, list of **additional** security attributes*
[326] Selection: *choose one of: restrictive, permissive, [assignment: other property]*

FMT_MSA.3.2/AK.TLS	The TSF shall allow the S_Administrator[327] to specify alternative initial values to override the default values when an object or information is created.
ST-Anwendungshinweis 46	Es gibt keine vom Administrator konfigurierbaren Anfangswerte für TLS-Verbindungen. Alle Konfigurationswerte für TLS Verbindungen sind durch [gemSpec_Krypt] vorgegeben und in der Firmware hart, vgl. die Darstellungen in Anhang B. Somit ist die Anforderung FMT_MSA.3.2/AK.TLS implizit erfüllt.

FTP_ITC.1/AK.FD

Inter-TSF trusted channel / Zum Fachdienst

FTP_ITC.1.1/AK.FD	The TSF shall provide a communication channel between itself and **a S_Fachdienst ~~another trusted IT product~~** that is logically distinct from other communication channels and provides assured identification of **S_Fachdienst mit dem Zertifikat C.FD.TLS-S mit dem Sperrstatus (OCSP) „good“[328] gegenüber dem EVG und EVG mit dem Zertifikat C.HCI.AUT gegenüber S_Fachdienst wenn von S_Fachmodul gefordert ~~its end points~~** and protection of the channel data from modification **and ~~or~~** disclosure.
FTP_ITC.1.2/AK.FD	The TSF shall permit *the TSF*[329] to initiate communication via the trusted channel
FTP_ITC.1.3/AK.FD	The TSF shall initiate communication via the trusted channel for die Bearbeitung von fachlichen Anwendungsfällen, die eine Online-Kommunikation mit Fachdiensten erfordern[330]
ST-Anwendungshinweis 47	„Fachdienst“ beinhaltet in diesem Zusammenhang auch den Intermediär, da der TOE keine unmittelbare Verbindung zum Fachdienst aufbaut.

FTP_ITC.1/AK.VZD

Inter-TSF trusted channel / Zum zentralen Verzeichnisdienst

FTP_ITC.1.1/AK.VZD	The TSF shall provide a communication channel between itself and **S_Verzeichnisdienst (VZD) ~~another trusted IT product~~** that is logically distinct from other communication channels and provides assured identification of **S_Verzeichnisdienst (VZD) mit dem Zertifikat C.ZD.TLS-S mit dem Sperrstatus (OCSP) „good“[331] gegenüber dem EVG ~~its end points~~** and protection of the channel data from modification **and ~~or~~** disclosure.

[327] Assignment: *the authorised identified roles*
[328] Refinement: *Gemäß Vorgaben aus TIP1-A_7254*
[329] Selection: *the TSF, another trusted IT product*
[330] Assignment: *list of functions for which a trusted channel is required*
[331] Refinement: *Gemäß Vorgaben aus TIP1-A_7254*

FTP_ITC.1.2/AK.VZD — The TSF shall permit *the TSF*[332] to initiate communication via the trusted channel.

FTP_ITC.1.3/AK.VZD — The TSF shall initiate communication via the trusted channel for MGM_LU_ONLINE=Enabled und MGM_LOGICAL_SEPARATION=Disabled des TUC_KON_290 „LDAP-Verbindung aufbauen“

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

FTP_ITC.1.1/AK.KSR — The TSF shall provide a communication channel between itself and **S_KSR**[333] ~~**another trusted IT product**~~ that is logically distinct from other communication channels and provides assured identification of **S_KSR mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG**[334] ~~**its end points**~~ and protection of the channel data from modification **and**[335] ~~**or**~~ disclosure.

FTP_ITC.1.2/AK.KSR — The TSF shall permit *the TSF*[336] to initiate communication via the trusted channel.

FTP_ITC.1.3/AK.KSR — The TSF shall initiate communication via the trusted channel for Prüfung auf neue Firmware-Update-Pakete und Download neuer Firmware-Update-Pakete[337].

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

FTP_ITC.1.1/AK.TSL — The TSF shall provide a communication channel between itself and **S_TSL_Dienst**[338] ~~**another trusted IT product**~~ that is logically distinct from other communication channels and provides assured identification of **S_TSL_Dienst mit dem Zertifikat C.ZD.TLS-S gegenüber dem EVG**[339] ~~**its end points**~~ and protection of the channel data from modification **and**[340] ~~**or**~~ disclosure.

FTP_ITC.1.2/AK.TSL — The TSF shall permit the TSF[341] to initiate communication via the trusted channel.

FTP_ITC.1.3/AK.TSL — The TSF shall initiate communication via the trusted channel for Download des BNetzA-VL Hashwerts und Download der BNetzA-VL **und Download des TSL-Hashwerts und Download der TSL**.

[332] Selection: *the TSF, another trusted IT product*
[333] Refinement
[334] Refinement
[335] Refinement
[336] Selection: *the TSF, another trusted IT product*
[337] Assignment: *list of functions for which a trusted channel is required*
[338] Refinement
[339] Refinement
[340] Refinement
[341] Assignment: *the TSF, another trusted IT product*

FTP_ITC.1/AK.CS

Inter-TSF trusted channel / Clientsystem

FTP_ITC.1.1/AK.CS	The TSF shall provide a communication channel between itself and a **Clientsystem in the LAN**[342] ~~**trusted IT product**~~ that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification **and**[343] ~~**or**~~ disclosure.
FTP_ITC.1.2/AK.CS	The TSF shall permit *the Clientsystem*[344] to initiate communication via the trusted channel.
FTP_ITC.1.3/AK.CS	The TSF shall initiate communication via the trusted channel for ANCL_TLS_MANDATORY = Enabled[345] **to the Clientsystem and reject or cancel a communication with the Clientsystem outside the TLS channel. This includes access to the service directory service.** ~~**A communication with the service directory service outside the TLS channel is only permitted if ANCL_DVD_OPEN is set to "Enabled".**~~[346]347

FTP_ITC.1/AK.eHKT

Inter-TSF trusted channel / eHKT

FTP_ITC.1.1/AK.eHKT	The TSF shall provide a communication channel between itself and another **eHealth-Kartenterminal**[348] ~~**trusted IT product**~~ that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification **and**[349] ~~**or**~~ disclosure. **Die TSF muss einen Keep-Alive-Mechanismus der TLS- Verbindung zu den eHealth-Kartenterminals implementieren.** [350]
FTP_ITC.1.2/AK.eHKT	The TSF shall permit *another trusted IT product*[351] **eHealth- Kartenterminal**[352] to initiate communication via the trusted channel
FTP_ITC.1.3/AK.eHKT	The TSF shall initiate communication via the trusted channel for Senden von SICCT-Kommandos an eHealth-Kartenterminals und Emp-

[342] Refinement
[343] Refinement
[344] Selection: *the TSF, another trusted IT product*
[345] Assignment: *list of functions for which a trusted channel is required*
[346] Deletion: *Vgl. ST-Anwendungshinweis 44*
[347] Refinement
[348] Refinement
[349] Refinement
[350] Refinement
[351] Selection: *the TSF, another trusted IT product*
[352] Refinement

fangen von SICCT-Antworten der eHealth-Kartenterminals an den EVG[353]

FDP_ITC.2/AK.BNetzA-VL
Import of user data / BNetzA-VL

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] hier erfüllt durch: FDP_ACC.1/AK.TLS [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] hier erfüllt durch: FTP_ITC.1/AK.TSL FPT_TDC.1 Inter-TSF basic TSF data consistency hier erfüllt durch: FPT_TDC.1/AK
FDP_ITC.2.1/AK.BNetzA-VL	The TSF shall enforce the **the parts of** AK-TLS-SFP **concerning BNetzA-VL**[354] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/AK.BNetzA-VL	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/AK.BNetzA-VL	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/AK.BNetzA-VL	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/AK.BNetzA-VL	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[355].

6.3.3.8. Sicherer Datenspeicher

FDP_ACC.1/AK.SDS
Subset access control / Sicherer Datenspeicher

FDP_ACC.1.1/AK.SDS	The TSF shall enforce the SDS-SFP[356] on subjects: (1) S_AK, (2) S_Fachmodul,

[353] Assignment: *list of functions for which a trusted channel is required*
[354] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[355] Assignment: *additional importation control rules*
[356] Assignment: *access control SFP*

(3) S_Administrator

objects:

(1) Schlüssel für sicheren Datenspeicher,

(2) Datenobjekte des sicheren Datenspeichers,

operations:

(1) lesen

(2) schreiben

.[357]

FDP_ACF.1/AK.SDS

Security attribute based access control / Sicherer Datenspeicher

FDP_ACF.1.1/AK.SDS

The TSF shall enforce the SDS-SFP[358] to objects based on the following:

subjects:

(1) S_AK,

(2) S_Fachmodul,

(3) S_Administrator

objects:

(1) Datenobjekte des sicheren Datenspeichers,

(2) Datenobjekte des sicheren Datenspeichers with security attribute Administratorobjekt.[359]

FDP_ACF.1.2/AK.SDS

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Das S_AK darf Datenobjekte im sicheren Datenspeicher nur verschlüsselt speichern.

(2) Das S_AK darf nach Inbetriebnahme des Konnektors die Datenobjekte des SDS mit dem Sicherheitsattribut „allgemeines Datenobjekt“ lesen, entschlüsseln und außerhalb des sicheren Datenspeichers nur temporär speichern,

(3) Das S_Fachmodul darf Daten an den S_AK übergeben und vom S_AK empfangen, die der S_AK als Datenobjekte des SDS mit dem Sicherheitsattribut „allgemeines Datenobjekt“ speichert,

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

[358] Assignment: *access control SFP*

[359] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

(4) Datenobjekte des SDS mit dem Sicherheitsattribut „Administratorobjekt“ darf nur innerhalb einer Administratorsitzung entschlüsselt und gelesen und verschlüsselt und geschrieben werden, aber nicht außerhalb der Administratorsitzung gespeichert werden,

(5) Keine weiteren Regeln[360].

ST-Anwendungshinweis 48

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

FDP_ACF.1.3/AK.SDS

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[361].

FDP_ACF.1.4/AK.SDS

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Das S_AK darf Datenobjekte des SDS mit dem Sicherheitsattribut „Adminstratorobjekt“ weder lesen noch entschlüsseln.

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

(3) none[362].

ST-Anwendungshinweis 49

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

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

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

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

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

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

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

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

6.3.3.9. Fachmodule

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

FDP_ACC.1.1/AK.VSDM — The TSF shall enforce the VSDM-SFP[363] on

subjects:

(1) S_AK,

(2) S_VSDM_Fachmodul,

(3) S_VSDM_Intermediär,

(4) S_VSDD_Fachdienst,

(5) S_CMS,

(6) S_eGK,

(7) S_Administrator;

objecte:

(1) Daten der Chipkarten (Versichertenstammdaten),

(2) Objektsystem der Chipkarte (eGK);

operations:

(1) Lesen der Versichertenstammdaten,

(2) Schreiben der Versichertenstammdaten,

(3) Ergänzen des Objektsystems

.[364]

[363] Assignment: *access control SFP*

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

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

FDP_ACF.1.1/AK.VSDM

The TSF shall enforce VSDM-SFP[365] to objects based on the following:

subjects:

(1) S_AK,

(2) S_VSDM_Fachmodul,

(3) S_VSDM_Intermediär,

(4) S_VSDD_Fachdienst,

(5) S_CMS,

(6) S_eGK;

objects:

(7) Daten der Chipkarten (Versichertenstammdaten) with the security attribute:

a) „geschützt“

b) „ungeschützt“

(8) Objektsystem der Chipkarte (eGK)

:[366]

FDP_ACF.1.2/AK.VSDM

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) Der S_VSDM_Fachmodul kommuniziert mit dem VSDD und dem CMS über den VSDM_Intermediär und fordert dafür den Bereitstellung eines TLS-Kanals mit gegenseitiger Authentisierung gemäß FTP_ITC.1/AK.FD durch S_AK an.

(2) Bei Zugriff des VSDD_Fachdienst oder des CMS auf die eGK ermöglicht S_VSDM_Fachmodul den Aufbau eines Secure Messaging Kanals zwischen VSDD_Fachdienst bzw. CMS und der eGK.

(3) Zugriffe auf S_eGK durch S_VSDD_Fachdienst werden vom S_AK (Chipkartendienst) auf dem Objektsystem der eGK protokolliert.

(4) Keine weiteren Regeln.[367]

FDP_ACF.1.3/AK.VSDM

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None[368].

[365] Assignment: *access control SFP*

[366] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*

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

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

FDP_ACF.1.4/AK.VSDM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None[369].

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

FMT_MSA.1.1/AK.VSDM	The TSF shall enforce the VSDM-SFP to restrict the ability to *no operation*[370] the security attributes none[371] to S_Administrator.
ST-Anwendungshinweis 50	Das PP definiert für das Subjekt S_VSDM_Fachmodul lediglich die Identität – also den eindeutigen Namen des Fachmoduls – als Sicherheitsattribut (vgl. [BSI-CC-PP-0098, Tabelle 12]). Neben der Identität werden keine weiteren Sicherheitsattribute für das Fachmodul VSDM definiert, die durch einen Administrator geändert werden können. Daher werden hier keine Operationen und keine Sicherheitsattribute operationalisiert.

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

FMT_MSA.3.1/AK.VSDM	The TSF shall enforce the VSDM-SFP[372] to provide *restrictive*[373] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AK.VSDM	The TSF shall allow the S_Administrator[374] to specify alternative initial values to override the default values when an object or information is created.
ST-Anwendungshinweis 51	Es gibt keine vom Administrator änderbaren Konfigurationswerte. Folglich können keine alternativen Anfangswerte definiert werden. Somit ist die Anforderung implizit erfüllt.

6.3.3.10. Übergreifende Sicherheitsanforderungen

FMT_MSA.4/AK
Security attribute value inheritance

FMT_MSA.4.1/AK	The TSF shall use the following rules to set the value of security attributes: (1) Der Chipkartendienst erzeugt für jede neu gesteckte Chipkarte (a) für identifizierte KVK,

[369] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[370] Selection: ***create**, change_default, query, modify, delete, [assignment: other operations]*
[371] Assignment: *list of security attributes*
[372] Assignment: *access control SFP, information flow control SFP*
[373] Selection: *choose one of: restrictive, permissive, [assignment: other property]*
[374] Assignment: *the authorised identified roles*

(b) für identifizierte eGK, SMC und HBA

ein Kartenhandle und übergibt das Kartenhandle und die damit verknüpften Informationen an das Subjekt S_AK.

(2) Der Chipkartendienst öffnet auf Anforderung des Subjekts S_AK für eine mit dem Kartenhandle identifizierten Chipkarte einen logischen Kanal.

(3) Die TSF weisen

(a) vom EVG importierten zu signierenden Daten,

(b) vom EVG importierten zu verschlüsselnden Daten,

(c) vom EVG zu entschlüsselnden Daten,

(d) dem vom EVG identifizierten Subjekt „S_Benutzer_Clientsystem“

die vom EVG übergebene Identität und den Autorisierungsstatus „nicht autorisiert“ zu.

(4) Die TSF weisen nach erfolgreicher Prüfung der Signatur-PIN der Signaturchipkarte des identifizierten Benutzers des Clientsystems dem Autorisierungsstatus des Subjektes S_Benutzer_Clientsystem den Wert „autorisiert“ zu.

(5) Die TSF weisen den zu signierenden Daten einer Liste nach erfolgreicher Prüfung der Signatur-PIN der Signaturchipkarte des S_Benutzer_Clientsystem den Autorisierungsstatus „autorisiert“ zu.

(6) Der AK setzt den Wert des Sicherheitsattributes „Ordnungsgemäßigkeit der Signatur“ aller signierten Daten eines autorisierten Signaturstapels, der von der QSEE gesendet wird, auf „ordnungsgemäß“, falls folgendes gilt:

(a) Das S_Benutzer_Clientsystem hat während der Signaturerstellung keinen Abbruch der Signatur gefordert.

(b) Die TSF empfangen für jedes Kommando zur Signaturerzeugung einen erfolgreichen Rückkehrcode der QSEE.

(c) Die Anzahl der signierten Dokumente entspricht der Anzahl der zum Signieren übersandten Dokumente des autorisierten Stapels.

(d) Die qualifizierten elektronischen Signaturen für alle Elemente des autorisierten Signaturstapels werden vom EVG erfolgreich mit dem zum festgelegten Zeitpunkt gültigen qualifizierten Zertifikat des Benutzers des Clientsystems verifiziert.

(e) Die qualifizierten elektronischen Signaturen beziehen sich auf den vorher identifizierten Benutzer des Clientsystems und die Daten des autorisierten Signaturstapels.

(f) Die Freischaltung der QSEE für die Erstellung von qualifizierten elektronischen Signaturen wurde von dem EVG erfolgreich zurückgesetzt**, wenn die Komfortsignatur für die QSEE nicht aktiviert ist**[375].

(g) Wenn die Komfortsignatur für die QSEE aktiviert ist, setzt der EVG den Wert des Sicherheitsattributes „Ordnungsgemäßigkeit der Signatur“ der signierten Daten bei Erfüllung von (6) (a)…(e) auf „ordnungsgemäß“, obwohl die Freischaltung der QSEE weiterhin besteht.[376]

Sollte einer dieser Punkte nicht erfüllt sein, erhalten alle signierten Dokumente, die durch die aktuelle Signatur-PIN-Eingabe autorisiert wurden, das Attribut „ungültig“.

(7) Der EVG weist den Wert des Sicherheitsattributes „Ordnungsgemäss verschlüsselt“ verschlüsselter Daten nur dann auf „ordnungsgemäß“, wenn

(a) die identifizierte Verschlüsselungsrichtlinie für die zu verschlüsselnden Daten gültig ist,

(b) zu den vorgesehenen Empfängern gültige Verschlüsselungszertifikate existieren und für die Verschlüsselung des symmetrischen Schlüssels verwendet wurden,

(c) die durch den Xpath-Ausdruck selektierten zu verschlüsselnden Daten vollständig verschlüsselt wurden und

(d) keine Fehler auftraten.

.

ST-Anwendungshinweis 52 Zur Interpretation des Begriffs „Verschlüsselungsrichtlinie“ vgl. ST-Anwendungshinweis 40.

FDP_RIP.1/AK

Subset residual information protection

FDP_RIP.1.1/AK The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[377] the following objects:

(1) geheime kryptographische Schlüssel,

(2) zu signierende Daten,

(3) signierte Daten (nach der Ausgabe),

(4) zu verschlüsselnde Daten (nach der Verschlüsselung),

[375] Refinement: *Gemäß Vorgaben aus A_18597*

[376] Refinement: *Gemäß Vorgaben aus A_18597*

[377] Selection: *allocation of the resource to, deallocation of the resource from*

(5) verschlüsselte Daten (nach der Ausgabe),

(6) vorgeschlagene Empfänger,

(7) entschlüsselte Daten (nach der Ausgabe),

(8) Benutzerdaten, die über den TLS-Kanal zwischen EVG und eHealth-Kartenterminals übermittelt wurden

.[378]

Daten einer eGK dürfen nicht über den Steckzyklus der Karte hinaus im EVG gespeichert werden. Daten von HBA und SM-B dürfen nicht länger als 24 Stunden im EVG zwischengespeichert werden.

Die sensitive Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. In jedem Fall müssen die sensitiven Daten vor dem Herunterfahren bzw. wenn möglich vor Reset, überschrieben werden.[379]

6.3.4. Klasse FMT: Sicherheitsmanagement

FMT_SMR.1/AK
Security roles

FMT_SMR.1.1/AK The TSF shall maintain the roles

(1) Administrator,

(2) Benutzer des Clientsystems,

(3) HBA,

(4) gSMC-KT, PIN-Sender,

(5) SMC-B,

(6) eGK,

(7) Kartenterminal,

(8) CMS of the gSMC-K,

(9) Clientsystem,

(10) Fachmodul,

(11) Fachdienst

.[380]

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

[378] Assignment: *list of objects*
[379] Refinement
[380] Assignment: *the authorised identified roles*

FMT_SMF.1/AK
Specification of Management Functions

FMT_SMF.1.1/AK

The TSF shall be capable of performing the following management functions:

(1) Manage eHealth-Kartenterminals according to FMT_MTD.1/AK.eHKT_Abf and FMT_MTD.1/AK.eHKT_Mod,

(2) Manage Arbeitsplatzkonfiguration with assigned Clientsystems and eHealth-Kartenterminals according to FMT_MTD.1/AK.Admin,

(3) Manage Signaturrichtlinien according to FMT_MSA.3/AK.Sig,

(4) Manage TLS-Kanäle according to FMT_MSA.3/AK.TLS,

(5) Manage Cross-CVC according to FMT_MTD.1/AK.Zert,

(6) Management of TSF functions according to FMT_MOF.1/AK

(7) Manage configuration parameters of Fachmodule

.[381]

FMT_MOF.1/AK
Management of security functions behaviour

FMT_MOF.1.1/AK

The TSF shall restrict the ability to *disable and enable*[382] the functions Online Kommunikation, Signaturdienst und Logische Trennung[383] to Administrator[384].

The following rules apply:

1. **If the attribute MGM_LU_ONLINE is set to "Disabled", the Konnektor never establishes an online connection. This means, the following services are deactivated in this case:**
   - **(1) Zertifikatsdienst: The TSL will be activated without evaluation of the revocation status (see FPT_TDC.1/AK).**
   - **(2) TLS connection for Fachdienste: no TLS communication according to FTP_ITC.1/AK.FD.**
   - **(3) Zeitdienst: time synchronization FPT_STM.1/NK.**
   - **(4) Software-Aktualisierungsdienst: no communication with the update server according to FDP_ACF.1.4/AK.Update.**

[381] Assignment: *list of management functions to be provided by the*
[382] Selection: *determine the behaviour of, disable, enable, modify the behaviour of*
[383] Assignment: *list of functions*
[384] Assignment: *the authorised identified roles*

2. **If the attribute MGM_LU_SAK is set to "Disabled", the Signaturdienst for QES according to the chapters 6.3.1.3 and 6.3.3.4 is deactivated.**
3. **If the logical separation is activated (attribute MGM_LOGICAL_SEPARATION set to "Enabled"), the following rules apply:**
   (1) If invoked from an external interface, the Verschlüsselungsdienst of the Konnektor must not check the revocation status of certificates.
   (2) If invoked from an external interface, the Signaturdienst of the Konnektor must not check the revocation status of certificates.
   (3) IF MGM_LU_ONLINE is not enabled, the NTP server of the Konnektor must be deactivated.
   (4) If MGM_LU_ONLINE is set to "Enabled", the Konnektor may only resolve the namespace „TI (*.DNS_TOP_LEVEL_DOMAIN_TI) " for internal services and internal Fachanwendungen and must not resolve this namespace for requests originatred from the LAN.
   (5) The Konnektor must block all communication on its external interfaces with the following systems:
      a. with systems in the network segment ANLW_AKTIVE_BESTANDSNETZE initiated by „Aktive Komponenten",
      b. with the Internet via SIS and IAG.[385]

ST-Anwendungshinweis 53 Die gematik Spezifikation sieht die Betriebseigenschaft *MGM_LOGICAL_SEPARATION* nicht länger vor [gemSpec_Kon]. Die logische Trennung ist nicht im TOE implementiert ist. Daher ist es nicht möglich, die Auswahl „logische Trennung" zu aktivieren.

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

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

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

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

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

[385] Refinement

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

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

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

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

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

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

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

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

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

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

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

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

(16) query the version information of Fachmodule,

(17) modify the connection parameters of Clientsysteme,

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

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

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

(21) import the O_Zertifikat_gSMC-K,

(22) select the TOE authentication certificate

to administrator.

ST-Anwendungshinweis 54 FMT_MTD.1.1/AK.Admin(5), (6) kommt in der Architektur des vorliegenden TOE nicht zum Tragen, vgl. FMT_MSA.3/AK.Sig.

ST-Anwendungshinweis 55 Der TOE unterstützt die automatische Anwendung von Update-Paketen gemäß A_18390 und A_18391.

ST-Anwendungshinweis 56 FMT_MTD.1.1/AK.Admin(12): Die Schlüssel des sicheren Datenspeichers werden beim ersten Start des Geräts – noch in der Fertigungsstraße – erzeugt und können ausschließlich im Rahmen des Werksresets neu generiert werden. Der TOE stellt kein Schlüsselzugriffsinterface bereit. Ein Werksreset wiederum kann nur vom Administrator ausgelöst werden. Somit ist (12) durch (14) implizit erfüllt.

ST-Anwendungshinweis 57 TIP1-A_7255 wird von FMT_MTD.1.1/AK.Admin(16) umgesetzt.

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

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

(1) *delete*[386] the public keys of the CVC root CA[387] to the CMS of the gSMC-K[388]**,**

(2) ***import and permanently store*[389] the public keys of the CVC root CA by the use of cross CVC[390] to S_AK[391]**[392].

ST-Anwendungshinweis 58 (1) Der TOE löscht keine öffentlichen Schlüssel der CVC Root CA auf der gSMC-K. Der TOE initiiert die Übernahme öffentlicher Schlüssel der CVC Root CA aus übergebenen Cross-CV-Zertifikaten durch die gSMC-K.

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

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

---

[386] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[387] Assignment: *list of TSF data*
[388] Assignment: *the authorised identified roles*
[389] Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*
[390] Assignment: *list of TSF data*
[391] Assignment: *the authorised identified roles*
[392] Refinement

6.3.5. Klasse FPT: Schutz der TSF

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

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

(1) Zertifikate für die Prüfung qualifizierter elektronischer Signaturen,

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

(3) X.509-Verschlüsselungszertifikate,

(4) CV-Zertifikate,

(5) Trust-service Status Listen **und deren Hashwerte**,

(6) Certificate Revocation Listen,

(7) BNetzA-VL und BNetzA-VL Hashwerte,

(8) Zulässigkeit importierter zu signierenden bzw. zu prüfender signierten Daten gemäß implementierten Signaturrichtlinien,

(9) *Signaturrichtlinie*[393],

(10) **Vom TSP in ihrer Laufzeit verlängerte X.509-Zertifikate (O_Zertifikat_gSMC-K)**

when shared between the TSF and another trusted IT product.

ST-Anwendungshinweis 59 — TIP1-A_5482-01 wird umgesetzt durch Unterpunkt FPT_TDC.1.1/AK(4).

ST-Anwendungshinweis 60 — Unterpunkt FPT_TDC.1.1/AK(6) wird ergänzt: Die digitale Signatur einer manuell importierten TSL oder eines manuell importierten TSL-Signer-CA Cross-Zertifikats muss auch dann geprüft werden, wenn sich der Konnektor im kritischen Betriebszustand *EC_TSL_Out_Of_Date_Beyond_Grace_Period* befindet.

FPT_TDC.1.2/AK — The TSF shall use the following rules

(1) Zertifikate für die qualifizierte elektronische Signatur müssen erfolgreich gemäß Kettenmodell bis zur bekannten und verifizierten BNetzA-VL erfolgreich geprüft sein.

(2) Die digitale Signatur der BNetzA-VL muss erfolgreich mit dem in der TSL enthaltenen öffentlichen Schlüssel zur Prüfung der BNetzA-VL geprüft sein und ist nur im angegebenen Gültigkeitszeitraum anwendbar.

[393] Selection: *Signaturrichtlinie, Verschlüsselungsrichtlinie*

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

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

(5) Die Gültigkeit der CVC gemäß [BSI-CC-PP-0082-2] muss nach dem Schalenmodell bis zu einer bekannten Wurzelinstanz erfolgreich geprüft sein.

(6) Die digitale Signatur über der TSL muss erfolgreich mit dem öffentlichen Schlüssel zur Prüfung von TSL erfolgreich geprüft sein und ist nur im angegebenen Gültigkeitszeitraum anwendbar.

(7) Die digitale Signatur über der Certificate Revocation List muss mit dem öffentlichen Schlüssel zur Prüfung von CRL erfolgreich geprüft sein.

(8) Ein neuer öffentlicher Schlüssel zur Prüfung von TSL und CRL darf nur durch eine gültige TSL verteilt werden.

(9) *für Signaturrichtlinie die Kette der Signaturen bis zu einer bekannten Wurzelinstanz und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen*[394].

(10) Falls bei einer Zertifikatsprüfung OCSP-Abfragen verwendet werden, muss die Festlegung zeitlicher Toleranzen in einer OCSP-Response, definiert in `GS-A_5215` [gemSpec_PKI, Abschnitt 9.1.2.2], bei der Interpretation verwendet werden.[395]

(11) Vor der Verwendung im Konnektor müssen in ihrer Laufzeit verlängerte Zertifikate vom Typ `C.NK.VPN`, `C.AK.AUT`, `C.SAK.AUT` (als Teil von `O_Zertifikat_gSMC-K`) durch eine Prüfung gemäß `TUC_KON_037` erfolgreich geprüft sein.[396]

(12) Vor der Verwendung im Konnektor müssen in ihrer Laufzeit verlängerte Zertifikate vom Typ `C.SAK.AUTD_CVC`, `C.CA_SAK.CS` (als Teil von `O_Zertifikat_gSMC-K`) durch eine

[394] Selection: *für Signaturrichtlinie die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Vereinbarkeit mit den Regeln für qualifizierte elektronische Signaturen prüfen, für Verschlüsselungsrichtlinie die Kette der Signaturen bis zu einem bekannten Vertrauensanker und die Zulässigkeit prüfen, weitere einschränkende Regeln für nicht-qualifizierte elektronische Signaturen*

[395] Refinement: *Gemäß Vorgaben aus `GS-A_5215`*

[396] Refinement: *Gemäß Vorgaben aus `A_21749-03`*

Prüfung gemäß A_21749-03, Standardablauf 3f) erfolgreich geprüft sein.[397]

when interpreting the TSF data from another trusted IT product.

FPT_FLS.1/AK
Failure with preservation of secure state

FPT_FLS.1.1/AK

The TSF shall preserve a secure state **according to [gemSpec_Kon, TAB_KON_504]** when the following types of failures occur:

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

(2) Keine weiteren Fehlerarten[398]

Failures occured during the self test of the TOE (see FPT_TST.1/AK.Run-time and FPT_TST.1/AK.Out-Of-Band) must trigger a blockage of the affected parts of the TSF.

FPT_TEE.1/AK
Testing of external entities

FPT_TEE.1.1/AK

The TSF shall run a suite of tests

(1) *beim Herstellen einer Kommunikation mit einem Gerät, das vorgibt, ein eHealth-Kartenterminal zu sein*[399] to check the fulfillment of das Gerät ist dem EVG als zulässiges eHealth- Kartenterminal im LAN des Leistungsrbringers bekannt, d. h. ein eHealth-Kartenterminal mit dem Pairing-Geheimnis und der beim Pairing gesteckten gültigen gSMC-KT.[400]

(2) ***bei der Meldung eines eHealth-Kartenterminals über das Stecken einer Chipkarte***[401] **to check the fulfillment of:**

(a) die gesteckte Chipkarte ist eine KVK.

(b) Die Chipkarte ist eine Chipkarte des identifizierten Kartentyps eGK, HBA, gSMC-KT oder SMC-B und keine KVK.[402]

(3) ***bei entfernter Eingabe von PIN- oder PUK***[403] **to check the fulfillment of:**

[397] Refinement: *Gemäß Vorgaben aus A_21749-03*
[398] Assignment: *list of additional types of failures in the TSF*
[399] Selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*
[400] Assignment: *List of properties of the external entities*
[401] Selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*
[402] Assignment: *List of properties of the external entities*
[403] Selection: *selection: during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*

(a) Zulässigkeit mit dem CVC mit Flag ’54’ für die Nutzung einer gSMC-KT als PIN-Sender für die entfernte PIN- Eingabe.

(b) Zulässigkeit für einen HBA oder einer SMC-B mit dem CVC Flag ’55’ für die Nutzung einer Chipkarte als PIN- Empfänger für die entfernte PIN-Eingabe.[404][405]

.

FPT_TEE.1.2/AK — If the test fails, the TSF shall

(1) keine weitere Kommunikation mit dem Gerät aufzunehmen und eine Fehlermeldung an den EVG zu geben.

(2) Wenn für eine Chipkarte die Testfolge des identifizierten Kartentyps, der keine KVK ist, und der geforderten Rolle fehlschlägt, ist der angeforderte Prozess abzubrechen und eine Fehlermeldung an den EVG zu geben.

(3) Wenn die gesteckte Chipkarte nicht als KVK, eGK, HBA, gSMC-KT oder SMC-B identifiziert werden kann, soll die TSF die unbekannte Karte kennzeichnen und weitere Aktionen mit dieser Karte verbieten[406].

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

FPT_TST.1.1/AK.Run-time — The TSF shall run a suite of self tests beim Anlauf und regelmäßig während des Normalbetriebs to demonstrate the correct operation of stored TSF executable code[407].

FPT_TST.1.2/AK.Run-time — The TSF shall provide authorised users with the capability to verify the integrity of stored TSF configuration data[408].

FPT_TST.1.3/AK.Run-time — The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[409].

ST-Anwendungshinweis 61 — Die Sicherheitsanforderung FPT_TST.1 existiert bereits in einer Iteration für den Netzkonnektor, vgl. FPT_TST.1/NK.

[404] Assignment: *list of properties of the external entities*
[405] Refinement
[406] Assignment: *action for unknown smart cards*
[407] Assignment: *parts of TSF*
[408] Assignment: *parts of TSF data*
[409] Assignment: *parts of TSF*

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

FPT_TST.1.1/AK.Out-Of-Band — The TSF shall run a suite of self tests **durch TSF-Komponenten mit integritätsgeschützt gespeichertem Code**[410] *beim Erstanlauf und auf Anforderung eines autorisierten Benutzers*[411] to demonstrate the correct operation of *TSF*[412].

FPT_TST.1.2/AK.Out-Of-Band — The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[413].

FPT_TST.1.3/AK.Out-Of-Band — The TSF shall provide authorised users with the capability to verify the integrity **des gespeicherten ausführbaren Codes** of the whole TSF[414].

FPT_STM.1/AK
Reliable time stamps

FPT_STM.1.1/AK — The TSF shall be able to provide reliable time stamps **für vom AK erzeugte Protokolleinträge (gemäß FAU_GEN.1/AK).**

Der AK greift auf die Echtzeituhr zurück, die in regelmäßigen Abständen und auf Anforderung des Administrators vom NK mit einem vertrauenswürdigen Zeitdienst synchronisiert wird[415].

6.3.6. Klasse FAU: Sicherheitsprotokollierung

FAU_GEN.1/AK
Audit data generation

FAU_GEN.1.1/AK — The TSF shall be able to generate an audit record of the following auditable events **des Anwendungskonnektors**:

a) Start-up and shutdown of the audit functions **des Anwendungskonnektors**;

b) All auditable events for the *not specified*[416] level of audit; and

c) **The following specified security-relevant auditable events:**

- Power on / Shut down (einschließlich der Art der ausgelösten Aktion, z. B. Reboot) des Anwendungskonnektors,

[410] Refinement
[411] 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]*
[412] Selection: *[assignment: parts of TSF], TSF*
[413] Selection: *[assignment: parts of TSF data], TSF data*
[414] Assignment: *parts of TSF mit gespeichertem ausführbarem TSF-Code*
[415] Refinement
[416] Selection: *choose one of: minimum, basic, detailed, not specified*

- Durchführung von Softwareupdates einschließlich nicht erfolgreicher Versuche des Anwendungskonnektors,
- Zeitpunkt von Änderungen der Konfigurationseinstellungen und Export/Import von Konfigurationsdaten des Anwendungskonnektors,
- kritische Betriebszustände wie in der Tabelle in FPT_FLS.1/AK aufgelistet des Anwendungskonnektors,
- Ereignisse vom Typ „Sec“ des Anwendungskonnektors,[417]
- Ereignisse vom Typ „Sec“ der Fachmodule[418].

FAU_GEN.1.2/AK

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

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

b) For each **specified** audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no further information[419].

ST-Anwendungshinweis 62

Anwendungshinweis 203 des Schutzprofils bildet die Brücke zu TIP1-A_4710-02. Diese Anforderung bestimmt, dass keine persönlichen oder medizinischen Daten protokolliert werden dürfen.

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

> FAU_GEN.1/AK beschreibt die Protokollfunktionen des Anwendungskonnektors in Ergänzung zu FAU_GEN.1/NK.SecLog. Die Protokoll-Daten dürfen keine personenbezogenen oder medizinischen Daten **oder Schlüsselmaterial** enthalten. Zum Nachweis dieser Anforderung für die Produktzulassung sind alle möglichen Protokoll-Einträge zu dokumentieren. Die Spezifikation Konnektor [gemSpec_Kon] gibt im Anhang F eine Übersicht der Ereignisse (Events), wobei nur die Beschreibungen der Ereignisse für die jeweiligen Technischen Anwendungsfülle (TUC) verbindlich sind.

[417] Assignment: *other specifically defined auditable events*
[418] Assignment: *additional events*
[419] Assignment: *other audit relevant information*

FAU_SAR.1/AK
Audit review

FAU_SAR.1.1/AK	The TSF shall provide users with role „administrator“[420] with the capability to read the system log and the security log[421] from the audit records.
FAU_SAR.1.2/AK	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1/AK
Protected audit trail storage

FAU_STG.1.1/AK	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2/AK	The TSF shall be able to *prevent*[422] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4/AK
Prevention of audit data loss

FAU_STG.4.1/AK	The TSF shall overwrite the oldest stored audit records and take no further action[423] if the audit trail is full. **The TOE reserves memory in the non-volatile NAND flash for the event log. If the size of the log exceeds 80% of the reserved memory, the TOE shall inform the administrator via the display.**
ST-Anwendungshinweis 63	Das Überschreiben des ältesten Log-Eintrags aus dem PP-Assignment wird durch die Konfigurationsparameter *LOG_DAYS* (für den Basiskonnektor) und *FM_<fmName>_LOG_DAYS* (für Fachmodule) gesteuert. Die Parameter geben an, nach wievielen Tagen Logeinträge frühestens überschrieben werden können. Sollte die diese Grenze an Tagen noch nicht erreicht sein und das Protokoll trotzdem voll sein, werden die ältesten Einträge gelöscht und der Konnektor wird spezifikationskonform in den Fehlerzustand *EC_LOG_OVERFLOW* versetzt.

6.3.7. VAU Protokoll

Im folgenden werden die Sicherheitsanforderungen definiert, die der Konnektor erfüllen muss, um den Zugriff auf den VAU-Server-Endpunkt der Dokumentenverwaltung bereitzustellen. Der Bezug zu den Anforderungen der Spezifikation wird in Unterabschnitt 7.3.1 hergestellt.

[420] Assignment: *authorised users*
[421] Assignment: *list of audit information*
[422] Selection: *choose one of: prevent, detect*
[423] Assignment: *other actions to be taken in case of audit storage failure*

FTP_ITC.1/VAU
Inter-TSF trusted channel / VAU

Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_ITC.1.1/VAU	The TSF shall provide a communication channel **VAU protocol according to [gemSpec_Krypt, Kap. 6]** between itself and ~~**another trusted IT product**~~ **VAU server endpoint** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification ~~**or**~~ **and** disclosure.
FTP_ITC.1.2/VAU	The TSF shall permit *the TSF*[424] to initiate communication via the ~~**trusted channel**~~ **VAU protocol**.
FTP_ITC.1.3/VAU	The TSF shall initiate communication via the ~~**trusted channel**~~ **VAU protocol** for communication with VAU server endpoint[425].
ST-Anwendungshinweis 64	Die redaktionellen Verfeinerungen am SFR-Text verdeutlichen die Forderung nach einer spezifikationskonformen Umsetzung des VAU-Protokolls durch den TOE. Der konkrete Bezug zu den einzelnen Anforderungen der gematik wird in Unterunterabschnitt 7.3.1.1 hergestellt.
ST-Anwendungshinweis 65	Der TOE baut einen VAU-Kanal 24 Stunden nach dem Aufbau wieder ab. Eine automatische Neuaushandlung der Verbindung findet nicht statt.

FCS_COP.1/VAU.Hash
Cryptographic operation/Hash

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier nicht erfüllt, da SHA keine Schlüssel verwendet. FCS_CKM.4 Cryptographic key destruction hier nicht erfüllt, da SHA keine Schlüssel verwendet.

[424] Selection: *the TSF, another trusted IT product*
[425] Assignment: *list of functions for which a trusted channel is required*

FCS_COP.1.1/VAU.Hash	The TSF shall perform hash value calculation[426] in accordance with a specified cryptographic algorithm SHA-1, SHA-256[427] and cryptographic key sizes none[428] that meet the following: FIPS PUB 180-4 [FIPS 180-4][429].
ST-Anwendungshinweis 66	SHA-1 darf nur im Rahmen von OCSP für die CertID-Struktur verwendet werden (entsprechend GS-A_5131 [gemSpec_Krypt]).

FCS_CKM.1/VAU
Cryptographic key generation/VAU

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/VAU.AES FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_CKM.1.1/VAU	The TSF shall generate cryptographic keys **for authenticated data encryption with AES-GCM-256**[430] in accordance with a specified cryptographic key generation algorithm mutually authenticated ECDH based on brainpoolP256r1, and HKDF with SHA-256[431] and specified cryptographic key sizes 256 bit[432] that meet the following: VAU protocol — gematik spec. [gemSpec_Krypt, Chapter 6] brainpoolP256r1 — RFC 5639 [RFC 5639], ECC — TR-03111 [TR-03111], ECDH — NIST-SP800-56A [NIST SP 800-56A], HKDF — RFC 5869 [RFC 5869], SHA — FIPS PUB 180-4 [FIPS 180-4] [433].
ST-Anwendungshinweis 67	Die Zufallswerte für die Schlüsselgenerierung werden vom sicheren Zufallsgenerator gemäß FCS_RNG.1/Hash_DRBG erzeugt.

[426] Assignment: *list of cryptographic operations*
[427] Assignment: *cryptographic algorithm*
SHA-256: gemäß mehrerer Anforderungen im VAU-Protokoll
SHA-1: Gemäß Vorgaben aus GS-A_5131
[428] Assignment: *cryptographic key sizes*
[429] Assignment: *list of standards*
[430] Refinement: *Gemäß Vorgaben aus A_16943-01*
[431] Assignment: *cryptographic key generation algorithm*
Gemäß Vorgaben aus A_16852-01, A_16943-01
[432] Assignment: *cryptographic key sizes*
Gemäß Vorgaben aus A_16943-01
[433] Assignment: *list of standards*

FCS_COP.1/VAU.ECDSA
Cryptographic operation/ECDSA

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: Siehe ST-Anwendungshinweis 68 FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/VAU.ECDSA	The TSF shall perform data authentication by verification of ECDSA signatures[434] in accordance with a specified cryptographic algorithm ECDSA in X.92 format with OID ecdsa-with-Sha256 with curve brainpoolP256r1[435] and cryptographic key sizes 256 bit[436] that meet the following: VAU protocol — gematik spec. [gemSpec_Krypt, Chapter 6.4], ECC parameters — TAB_Krypt_002a [gemSpec_Krypt, Chapter 2.1.1.1], brainpoolP256r1 — RFC 5639 [RFC 5639], ECC — TR-03111 [TR-03111, Chapter 5.2.2], DSS — FIPS PUB 186-4 [FIPS 186-4], SHA — FIPS PUB 180-4 [FIPS 180-4] [437].
ST-Anwendungshinweis 68	Die *signature creation* wird von der SM-B oder von der eGK durchgeführt und liegt somit in der Umgebung des TOE. Die *verification of digital signatures* wird im TOE durchgeführt. Die Interpretation von VAU-Server-Zertifikaten wird durch FPT_TDC.1/VAU.Zert erbracht. Diese Argumentation folgt derjenigen des Schutzprofils in der Erklärung der Abhängigkeiten zu FCS_COP.1/NK.TLS.Auth.

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

Hierarchical to:	No other components
Dependencies:	No dependencies

[434] Assignment: *list of cryptographic operations*
Gemäß Vorgaben aus A_16941-01
[435] Assignment: *cryptographic algorithm*
Gemäß Vorgaben aus GS-A_4357-02
[436] Assignment: *cryptographic key sizes*
Gemäß Vorgaben aus GS-A_4357-02
[437] Assignment: *list of standards*

FPT_TDC.1.1/VAU.Zert — The TSF shall provide the capability to consistently interpret X.509 certificates of VAU server endpoint and the TSL[438] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/VAU.Zert — The TSF shall use Prüfkriterien:

(1) die Gültigkeitsdauer eines Zertifikates,

(2) Felder des Zertifikats mit Profil C.FD.AUT gemäß Tab_PKI_275 [gemSpec_PKI]:

CertificatePolicies::policyIdentifier	oid_policy_gem_or_cp
CertificatePolicies::policyIdentifier	oid_fd_aut
KeyUsage	DigitalSignature
ExtendedKeyUsage	(leer)
Admission::professionOID	oid_epa_vau (gemäß GS-A_4446-05)

(3) ob ein Zertifikat in einer gültigen Zertifikatskette bis zu einer zulässigen CA in der TSL enthalten ist,

(4) Sperrstatus per OCSP-Anfrage[439]

when interpreting the TSF data from ~~**another trusted IT product**~~ **VAU server endpoint**.

ST-Anwendungshinweis 69 — Das hier verwendete OCSP-Protokoll verwendet die Hash-Funktion SHA-1. Die Verwendung dieses Algorithmus erfolgt gemäß den Vorgaben aus GS-A_5131 [gemSpec_Krypt] hervor.

FCS_COP.1/VAU.AES
Cryptographic operation/AES für VAU

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
hier erfüllt durch: FCS_CKM.1/VAU
FCS_CKM.4 Cryptographic key destruction
hier erfüllt durch: FCS_CKM.4/AK

FCS_COP.1.1/VAU.AES — The TSF shall perform authenticated symmetric encryption and decryption[440] in accordance with a specified cryptographic algorithm AES-GCM with tag length 128 bit **and 96 bit initialization vector created by secure RNG according to FCS_RNG.1/Hash_DRBG**[441]

[438] Assignment: *list of TSF data types*
Gemäß Vorgaben aus A_16941-01
[439] Assignment: *list of interpretation rules to be applied by the TSF*
Gemäß Vorgaben aus GS-A_4652-01
[440] Assignment: *list of cryptographic operations*
Gemäß Vorgaben aus A_17070-02, A_17084, A_16945-02
[441] Assignment: *cryptographic algorithm*
Gemäß Vorgaben aus A_17070-02, GS-A_5016

and cryptographic key sizes 256 bit[442] that meet the following: FIPS PUB 197 [FIPS 197], NIST-SP800-38D [NIST SP 800-38D][443].

6.3.8. SGD Protokoll / ECIES Verfahren

Im folgenden werden die Sicherheitsanforderungen definiert, die der Konnektor erfüllen muss, um den Zugriff auf das SGD-HSM bereitzustellen. Der Bezug zu den Anforderungen der Spezifikation wird in Unterabschnitt 7.3.2 hergestellt.

FTP_ITC.1/SGD
Inter-TSF trusted channel / SGD

Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_ITC.1.1/SGD	The TSF shall provide a communication channel **according to section 2.3 of [gemSpec_SGD_ePA]** between itself and ~~**another trusted IT product**~~ **SGD-HSM** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification ~~**or**~~ **and** disclosure.
FTP_ITC.1.2/SGD	The TSF shall permit *the TSF*[444] to initiate communication via the trusted channel.
FTP_ITC.1.3/SGD	The TSF shall initiate communication via the trusted channel for accessing keys stored in SGD-HSM of SGD 1 and SGD 2[445].
ST-Anwendungshinweis 70	Die redaktionellen Verfeinerungen am SFR-Text verdeutlichen die Forderung nach einer spezifikationskonformen Umsetzung des SGD-Protokolls durch den TOE. Der konkrete Bezug zu den einzelnen Anforderungen der gematik wird in Unterunterabschnitt 7.3.2.1 hergestellt.

FCS_COP.1/SGD.Hash
Cryptographic operation/Hash

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]

[442] Assignment: *cryptographic key sizes*
[443] Assignment: *list of standards*
[444] Selection: *the TSF, another trusted IT product*
[445] Assignment: *list of functions for which a trusted channel is required*

	hier nicht erfüllt, da SHA keine Schlüssel verwendet. FCS_CKM.4 Cryptographic key destruction hier nicht erfüllt, da SHA keine Schlüssel verwendet.
FCS_COP.1.1/SGD.Hash	The TSF shall perform hash value calculation[446] in accordance with a specified cryptographic algorithm SHA-256[447] and cryptographic key sizes none[448] that meet the following: FIPS PUB 180-4 [FIPS 180-4][449].

FDP_ITC.2/SGD
Import of user data with security attributes / SGD

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] hier erfüllt durch: FDP_ACC.1/SGD [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] hier erfüllt durch: FTP_ITC.1/SGD FPT_TDC.1 Inter-TSF basic TSF data consistency hier erfüllt durch: FPT_TDC.1/SGD.Zert
FDP_ITC.2.1/SGD	The TSF shall enforce the SGD public key import SFP[450] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/SGD	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/SGD	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/SGD	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/SGD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: Import of public ECIES key from SGD-HSM by *getPublicKey* operation[451].

[446] Assignment: *list of cryptographic operations*
[447] Assignment: *cryptographic algorithm*
[448] Assignment: *cryptographic key sizes*
[449] Assignment: *list of standards*
[450] Assignment: *access control SFP(s) and/or information flow control SFP(s)*
[451] Assignment: *additional importation control rules*
Gemäß Vorgaben aus A_17897

FDP_ACC.1/SGD
Subset access control / SGD

Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control hier erfüllt durch: FDP_ACF.1/SGD
FDP_ACC.1.1/SGD	The TSF shall enforce the SGD public key import SFP[452] on subject S_AK, object public ECIES key of SGD-HSM, operation import[453].

FDP_ACF.1/SGD
Access control functions / SGD

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control hier erfüllt durch: FDP_ACC.1/SGD FMT_MSA.3 Static attribute initialisation hier erfüllt durch: ST-Anwendungshinweis 71
FDP_ACF.1.1/SGD	The TSF shall enforce the SGD public key import SFP[454] to objects based on the following: subject S_AK, object public ECIES key of SGD-HSM with security attributes ECDSA signature and certificate, operation import[455].
FDP_ACF.1.2/SGD	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Subject S_AK may import object public ECIES key of SGD-HSM only upon (1) successful verification of security attribute certificate according to FPT_TDC.1/SGD.Zert, and (2) successful verification of security attribute ECDSA signature according to FCS_COP.1/SGD.ECDSA [456].
FDP_ACF.1.3/SGD	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[457].

[452] Assignment: *access control SFP*
[453] Assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*
[454] Assignment: *access control SFP*
[455] Assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*
[456] Assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
Gemäß Vorgaben aus A_18024
[457] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*

FDP_ACF.1.4/SGD	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: public ECIES key of SGD-HSM may not be imported by S_AK except for accessing SGD-HSM with SGD protocol[458].
ST-Anwendungshinweis 71	Die Abhängigkeit zu FMT_MSA.3 ist nicht erfüllt: Für das Datenobjekt „public ECIES key of SGD-HSM“ findet keine Initialisierung von Sicherheitsattributen im Sinne von FMT_MSA.3 statt: ECIES-Schlüssel, Signatur und Zertifikat können vom TOE nicht sinnvoll mit Defaultwerten initialisiert werden.

FCS_COP.1/SGD.ECDSA
Cryptographic operation/ECDSA

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FDP_ITC.2/SGD FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/SGD.ECDSA	The TSF shall perform data authentication by verification of ECDSA signatures[459] in accordance with a specified cryptographic algorithm ECDSA in X.92 format with OID ecdsa-with-Sha256 with curve brainpoolP256r1[460] and cryptographic key sizes 256 bit[461] that meet the following: SGD protocol: gematik spec. [gemSpec_SGD_ePA, Chapters 2.3, 6], ECC parameters: TAB_Krypt_002a [gemSpec_Krypt, Chapter 2.1.1.1], brainpoolP256r1: RFC 5639 [RFC 5639], ECC: TR-03111 [TR-03111, Chapter 5.2.2], DSS: FIPS PUB 186-4 [FIPS 186-4], SHA: FIPS PUB 180-4 [FIPS 180-4] [462].
ST-Anwendungshinweis 72	Die *signature creation* wird von der SM-B oder von der eGK durchgeführt und liegt somit in der Umgebung des TOE. Allerdings muss der Konnektor bei der Erstellung der Signaturen in Abhängigkeit von der

[458] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*
[459] Assignment: *list of cryptographic operations*
Gemäß Vorgaben aus A_18024
[460] Assignment: *cryptographic algorithm*
Gemäß Vorgaben aus GS-A_4357-02
[461] Assignment: *cryptographic key sizes*
Gemäß Vorgaben aus GS-A_4357-02
[462] Assignment: *list of standards*

verwendeten Kartengeneration das richtige Signaturverfahren durchsetzen:

- G 2.0: Solche Karten beherrschen ausschließlich RSA-basierte Verfahren. Der TOE muss diese Kartengeneration und das geeignete Signaturverfahren unterstützen. Der Konnektor muss das korrekte Verfahren RSASSA-PSS durchsetzen.
- G 2.1: Solche Karten unterstützen auch ECDSA. Der TOE muss sicherstellen, dass bei solchen Karten ausschließlich ECDSA-Signaturen erzeugt werden.

Die *verification of digital signatures* wird im TOE durchgeführt. Die Interpretation von SGD-HSM-Zertifikaten wird durch FPT_TDC.1/SGD.Zert erbracht.

Diese Argumentation folgt derjenigen des Schutzprofils in der Erklärung der Abhängigkeiten zu FCS_COP.1/NK.TLS.Auth.

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

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_TDC.1.1/SGD.Zert	The TSF shall provide the capability to consistently interpret X.509 certificates of SGD-HSM and the TSL[463] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/SGD.Zert	The TSF shall use Prüfkriterien: (1) ob das Zertifikat in einer „Whitelist“ der EE-Zertifikate in der TSL innerhalb eines „TSPService“-Eintrags mit dem *ServiceTypeIdentifier* `http://uri.etsi.org/TrstSvc/Svctype/unspecified` aufgeführt ist, und ob dieses zeitlich aktuell gültig ist, (2) ob die Zertifikate die vorgeschriebenen OIDs gemäß Spezifikation [gemSpec_OID] enthalten: • Für SGD 1: oid_sgd1_hsm • Für SGD 2: oid_sgd2_hsm [464] when interpreting the TSF data from ~~another trusted IT product~~ **Schlüsselgenerierungsdienst**.

[463] Assignment: *list of TSF data types*
Gemäß Vorgaben aus A_18024
[464] Assignment: *list of interpretation rules to be applied by the TSF*
Gemäß Vorgaben aus A_18024

FCS_COP.1/SGD.ECIES
Cryptographic operation / ECIES

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FDP_ITC.2/SGD, FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4/AK
FCS_COP.1.1/SGD.ECIES	The TSF shall perform ECIES-based authenticated hybrid encryption and decryption[465] in accordance with a specified cryptographic algorithm ECIES with authenticated ECDH based on brainpoolP256r1, HKDF with SHA-256, and AES-GCM-256 with tag length 128 bit and 96 bit initialization vector created by secure RNG according to FCS_RNG.1/Hash_DRBG[466] and cryptographic key sizes 256 bit[467] that meet the following: ECIES [SEC1-2009], brainpoolP256r1 RFC 5639 [RFC 5639], ECC TR-03111 [TR-03111], ECDH NIST-SP800-56A [NIST SP 800-56A], HKDF RFC 5869 [RFC 5869], SHA FIPS PUB 180-4 [FIPS 180-4], AES FIPS PUB 197 [FIPS 197], GCM NIST-SP800-38D [NIST SP 800-38D] [468].
ST-Anwendungshinweis 73	Den *öffentlichen Schlüssel des Peers* für das hybride ECIES-Verfahren erhält der TOE durch die Umsetzung des ersten (und vierten) Schritts des SGD-Protokolls, wie in FTP_ITC.1/SGD gefordert. Die Abfolge der Schritte und der Bezug zu den jeweiligen SFR ist in ASE_TSS Unterabschnitt 7.3.2 beschrieben. Der Import des öffentlichen Schlüssels des Peers wird durch die SFR FCS_COP.1/SGD.ECDSA und FPT_TDC.1/SGD.Zert erfüllt. Das SGD-Protokoll schreibt vor, dass der öffentliche ECIES-Schlüssel vom SGD signiert wird. Der TOE prüft die Signatur in FCS_COP.1/SGD.ECDSA und das Signer-Zertifikat in FPT_TDC.1/SGD.Zert.

[465] Assignment: *list of cryptographic operations*
Gemäß Vorgaben aus A_17875
[466] Assignment: *cryptographic algorithm*
Gemäß Vorgaben aus A_17872, A_17874, A_17875, and GS-A_5016
[467] Assignment: *cryptographic key sizes*
Gemäß Vorgaben aus A_17875
[468] Assignment: *list of standards*

ST-Anwendungshinweis 74

Der Empfänger einer über das ECIES-Verfahren verschlüsselten Nachricht muss prüfen, ob der vom Sender erzeugte ephemere ECC-Punkt auf der gleichen elliptischen Kurve wie der Empfänger-ECC-Punkt liegt.

6.4. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

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

6.4.1. Verfeinerung zur Vertrauenswürdigkeitskomponente ADV_ARC.1

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

6.4.2. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_OPE.1

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

6.4.3. Verfeinerung zur Vertrauenswürdigkeitskomponente ALC_DEL.1

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

6.4.4. Verfeinerung zur Vertrauenswürdigkeitskomponente AGD_PRE.1

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

6.4.5. Verfeinerung für die Integration der Fachmodule NFDM, AMTS und ePA

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

> **Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 [TR-03154], TR-03155 [TR-03155] (jeweils Kapitel 3.3.2) und TR-03157 [TR-03157] (Kapitel 3.2.2) werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die für die Fachmodule NFDM, AMTS und ePA relevanten Sicherheitseigenschaften des Konnektors müssen zusätzlich im Security Target des Konnektors aufgenommen werden.**
>
> **Der *Hersteller* muss im Security Target beschreiben, dass der Konnektor die nach TR-03154 [TR-03154], TR-03155 [TR-03155] (jeweils Kapitel 3.3.2) und TR-03157 [TR-03157] (Kapitel 3.2.2) relevanten Sicherheitseigenschaften des Konnektors umsetzt.**
>
> **Der *Evaluator* muss prüfen, ob die nach TR-03154 [TR-03154], TR-03155 [TR-03155] (jeweils Kapitel 3.3.2) und TR-03157 [TR-03157] (Kapitel 3.2.2) relevanten Sicherheitseigenschaften des Konnektors vollständig im Security Target berücksichtigt sind.**

ADV_FSP wird wie folgt verfeinert:

Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 [TR-03154], TR-03155 [TR-03155] (jeweils Kapitel 3.3.2) und TR-03157 [TR-03157] (Kapitel 3.2.2) werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die dabei von den Fachmodulen aufgerufenen Schnittstellen des Anwendungskonnektors müssen beschrieben werden.

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

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

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

Der Konnektor unterstützt die Fachmodule NFDM, AMTS und ePA. In den Technischen Richtlinien TR-03154 [TR-03154], TR-03155 [TR-03155] (jeweils Kapitel 3.3.2) und TR-03157 [TR-03157] (Kapitel 3.2.2) werden Anforderungen an den Konnektor gestellt, die im Rahmen der CC-Zertifizierung berücksichtigt werden müssen. Die sichere und korrekte Umsetzung der relevanten Sicherheitseigenschaften muss geprüft werden.

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

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

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

6.5. Erklärung der Sicherheitsanforderungen

6.5.1. Erklärung der Abhängigkeiten der 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 6.5 aufgeführt.

6.5.2. 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 6.6 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 6.6.: Abbildung der Sicherheitsziele des NK auf *eigene* Sicherheitsanforderungen

6.5.3. Detaillierte Erklärung für die Sicherheitsziele des Netzkonnektors

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

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 6.5.: Abhängigkeiten der hinzugefügten SFR des Netzkonnektors

6.5.4. Erklärung der Abhängigkeiten der SFR des Anwendungskonnektors

Die Abhängigkeiten der in Abschnitt 6.3 aufgestellten funktionalen Sicherheitsanforderungen sind erfüllt. Es gelten dieselben Auflösungen von Abhängigkeiten, wie sie im Schutzprofil [BSI-CC-PP-0098, Abschnitt 6.5.2] beschrieben sind. Für die hinzugefügten SFR für PTV 5+ gelten die in Tabelle 6.7 beschriebenen Abhängigkeiten.

SFR	Abhängig von	Erfüllt durch
FCS_COP.1/AK.SigVer.BNetzA-VL	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2/AK.BNetzA-VL FCS_CKM.4/AK
FDP_ITC.2/AK.BNetzA-VL	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1/AK.TLS FTP_ITC.1/AK.TSL FPT_TDC.1/AK
FIA_API.1/AK.TLS	Keine Abhängigkeiten	–
FIA_SOS.1/AK.CS.Passwörter	Keine Abhängigkeiten	–
FTP_ITC.1/VAU	Keine Abhängigkeiten	–
FCS_COP.1/VAU.Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	–† –†
FCS_CKM.1/VAU	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/VAU.AES FCS_CKM.4/AK
FCS_COP.1/VAU.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	ST-Anwendungshinweis 68 FCS_CKM.4/AK
FPT_TDC.1/VAU.Zert	Keine Abhängigkeiten	–
FCS_COP.1/VAU.AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/VAU FCS_CKM.4/AK
FTP_ITC.1/SGD	Keine Abhängigkeiten	–
FCS_COP.1/SGD.Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	–† –†
FDP_ITC.2/SGD	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1/SGD FTP_ITC.1/SGD FPT_TDC.1/SGD.Zert
FDP_ACC.1/SGD	FDP_ACF.1	FDP_ACF.1/SGD
FDP_ACF.1/SGD	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/SGD ST-Anwendungshinweis 71

† Nicht erfüllt, da Hash-Algorithmen keine Schlüssel verwenden

SFR	Abhängig von	Erfüllt durch
FCS_COP.1/SGD.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2/SGD FCS_CKM.4/AK
FPT_TDC.1/SGD.Zert	Keine Abhängigkeiten	–
FCS_COP.1/SGD.ECIES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2/SGD FCS_CKM.4/AK
FCS_COP.1/AK.ECIES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2/AK.Enc FCS_CKM.4/AK

Tabelle 6.7.: Abhängigkeiten der hinzugefügten SFR

6.5.5. Überblick der Abdeckung von Sicherheitszielen des Anwendungskonnektors

Die Zuordnung von Sicherheitszielen zu Sicherheitsanforderungen des Anwendungskonnektors entspricht der Zuordnung, die im Schutzprofil getroffen wurde [BSI-CC-PP-0098, Abschnitt 6.5.4]. Einige Sicherheitsziele werden zusätzlich durch hinzugefügte SFR erfüllt. Weiterhin wurde durch die Funktionalität ePA das Sicherheitsziel O.AK.VAUSGD aufgenommen. Dieses Sicherheitsziel wird durch ebenfalls herstellereigene SFR abgedeckt. Tabelle 6.8 zeigt die Abdeckung der Sicherheitsziele *ausschließlich* durch die herstellereigenen SFR.

Das im Rahmen der Umsetzung der Komfortsignatur eingefügte Sicherheitsziel O.AK.Sig.Komfortsignatur wird durch Refinements an den bestehenden SFR FDP_ACF.1.2/AK.Sgen (4) (h),(i) und FMT_MSA.4.1/AK (6) (g) erfüllt.

	O.AK.Admin	O.AK.Basis_Krypto	O.AK.Chipkartendienst	O.AK.Dec	O.AK.Enc	O.AK.EVG_Modifikation	O.AK.exklusivZugriff	O.AK.IFD-Komm	O.AK.Infomodell	O.AK.LAN	O.AK.PinManagement	O.AK.Protokoll	O.AK.Selbsttest	O.AK.Sig.Einfachsignatur	O.AK.Sig.exklusivZugriff	O.AK.Sig.Komfortsignatur	O.AK.Sig.PrüfungZertifikat	O.AK.Sig.Schlüsselinhaber	O.AK.Sig.SignaturVerifizierung	O.AK.Sig.SignNonQES	O.AK.Sig.SignQES	O.AK.Sig.Stapelsignatur	O.AK.Update	O.AK.VAD	O.AK.VAUSGD	O.AK.VSDM	O.AK.VZD	O.AK.WAN	O.AK.Zeit
FCS_CKM.1/VAU	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.ECIES	.	.	.	✓	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.BNetzA-VL	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/SGD.ECDSA	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/SGD.ECIES	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/SGD.Hash	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/VAU.AES	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/VAU.ECDSA	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/VAU.Hash	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACC.1/SGD	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACF.1/SGD	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ITC.2/AK.BNetzA-VL	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ITC.2/SGD	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FIA_API.1/AK.TLS	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FIA_SOS.1/AK.CS.Passwörter	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FPT_TDC.1/SGD.Zert	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FPT_TDC.1/VAU.Zert	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FTP_ITC.1/SGD	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FTP_ITC.1/VAU	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.

Tabelle 6.8.: Abbildung der Sicherheitsziele des AK auf *eigene* Sicherheitsanforderungen

6.5.6. Detaillierte Erklärung für die Sicherheitsziele des Anwendungskonnektors

Die detaillierte Erklärung der Sicherheitsziele des Anwendungskonnektors wird unverändert aus [BSI-CC-PP-0098] übernommen. Für das hinzugefügte Sicherheitsziel für das Fachmodul ePA gilt zusätzlich folgende Erklärung:

6.5.6.1. O.AK.VAUSGD

Aspekt „Sicherer Kanal zum VAU-Server-Endpunkt“

In O.AK.VAUSGD fordert das Security Target abhörsichere Verbindungen zur vertrauenswürdigen Ausführungsumgebung der Dokumentenverwaltung. Genau dies leistet FTP_ITC.1/VAU. Die Refinements am SFR verweisen auf die Stelle der gematik-Spezifikation, an der das VAU-Protokoll definiert wird und ersetzen den generischen Endpunkt „another trusted IT product“ durch den protokollspezifischen Endpunkt. Damit wird Protokollkonformität gefordert. Das SFR steht somit stellvertretend für alle gematik-Anforderungen an den Ablauf des Protokolls.

Der Kernpunkt des Protokolls ist aus Sicht dieses Security Targets die Aushandlung kryptographischer Geheimnisse und die Verwendung kryptographischer Algorithmen. Besonderer Fokus liegt auf der Schlüsselaushandlung. Hierfür wird eine einzelne Sicherheitsanforderung modelliert: FCS_CKM.1/VAU leitet aus dem empfangenen öffentlichen Schlüssel und dem eigenen Geheimnis mittels ECDHE ein shared secret ab. Anschließend werden mit der HKDF die in der Spezifikation geforderten AES-Schlüssel abgeleitet. Das in diesem Kontext erhaltene Zertifikat wird mit den Regeln aus FPT_TDC.1/VAU.Zert geprüft. Die Signatur des Zertifikats wird mit FCS_COP.1/VAU.ECDSA verifiziert. Die im Protokoll geforderte Berechnung von Hashwerten erfolgt durch FCS_COP.1/VAU.Hash. Die Daten im VAU-Kanal werden gemäß FCS_COP.1/VAU.AES ver- und entschlüsselt. Alle Zufallszahlen, die für den sicheren Kanal zum VAU-Server-Endpunkt benötigt werden, stammen aus dem sicheren Zufallsgenerator nach FCS_RNG.1/Hash_DRBG. Die Schlüsselvernichtung übernimmt FCS_CKM.4/AK.

Aspekt „Sicherer Kanal zum Schlüsselgenerierungsdienst“

In O.AK.VAUSGD fordert das Security Target abhörsichere Verbindungen zum Schlüsselgenerierungsdienst. Genau dies leistet FTP_ITC.1/SGD. Die Refinements am SFR verweisen auf die Stelle der gematik-Spezifikation, an der das ECIES-Protokoll definiert wird und ersetzen den generischen Endpunkt „another trusted IT product“ durch den protokollspezifischen Endpunkt. Damit wird Protokollkonformität gefordert. Das SFR steht somit stellvertretend für alle gematik-Anforderungen an den Ablauf des Protokolls.

Der Kernpunkt des Protokolls ist aus Sicht dieses Security Targets die Aushandlung kryptographischer Geheimnisse und die Verwendung kryptographischer Algorithmen. Besonderer Fokus liegt auf dem ECIES-Verfahren. Hierbei finden zwei Aspekte Beachtung: der Import des öffentlichen Schlüssels des SGD-HSM und die Verschlüsselung inklusive der Schlüsselableitung.

Für den Import wird die Sicherheitsanforderung FDP_ITC.2/SGD modelliert. Sie sorgt dafür, dass der öffentliche ECIES-Schlüssel über die Operation *getPublicKey* des SGD-Protokolls in den TOE eingebracht wird. Der Import und die Verwendung des Schlüssels unterliegt der SGD public key import SFP. Hierfür werden die Sicherheitsanforderungen FDP_ACC.1/SGD und FDP_ACF.1/SGD definiert. Diese wiederum fordern die Verifikation des Zertifikats gemäß den Interpretationsregeln in FPT_TDC.1/SGD.Zert und die Validierung der Signatur mit FCS_COP.1/SGD.ECDSA.

Für die Verschlüsselung wird eine einzelne Sicherheitsanforderung modelliert: FCS_COP.1/SGD.ECIES leitet aus dem empfangenen öffentlichen Schlüssel des SGD-HSM und dem eigenen Geheimnis mittels

ECDH ein shared secret ab. Anschließend werden mit der HKDF die in der Spezifikation geforderten AES-Schlüssel abgeleitet. Dieser Schlüssel wird für das ECIES-Verfahren verwendet. Die im Protokoll geforderte Berechnung von Hashwerten erfolgt durch FCS_COP.1/SGD.Hash. Alle Zufallszahlen, die für den sicheren Kanal zum SGD-HSM benötigt werden, stammen aus dem sicheren Zufallsgenerator nach FCS_RNG.1/Hash_DRBG. Die Schlüsselvernichtung übernimmt FCS_CKM.4/AK.

6.6. Erklärung für Erweiterung der Sicherheitsanforderungen

FCS_RNG.1/Hash_DRBG
Die Sicherheitsanforderung FCS_RNG.1/Hash_DRBG wurde eingeführt, um die Anforderungen der ebenfalls eingeführten Komponente FCS_RNG.1 zu präzisieren. Die Erklärung für die Einführung der Familie FCS_RNG in Abschnitt 5.1 gilt auch für das resultierende SFR FCS_RNG.1/Hash_DRBG. Die Sicherheitsanforderung erfüllt das Sicherheitsziel O.NK.TLS_Krypto, vgl. auch Unterabschnitt 6.5.1. Ebenso erfüllt das SFR das Sicherheitsziel O.AK.Basis_Krypto bei der Erstellung von AES-Schlüsseln.

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

FCS_COP.1/AK.SigVer.BNetzA-VL
FCS_COP.1/AK.SigVer.BNetzA-VL wurde eingeführt, um die Algorithmen des TOE zur Verifikation der Signatur der BNetzA-VL zu repräsentieren. Diese Anforderung wird auf das Sicherheitsziel O.AK.Sig.PrüfungZertifikat abgebildet, in Einklang mit der Zuordnung von FPT_TDC.1/AK. Dieses SFR beschreibt die Interpretation der BNetzA-VL. Die Verifikation der Zertifikatssignatur ist ein Teil der Interpretation der Vertrauensliste. Somit ist das neue SFR demselben Sicherheitsziel zugeordnet.

FDP_ITC.2/AK.BNetzA-VL
FDP_ITC.2/AK.BNetzA-VL wurde eingeführt, um den Import der BNetzA-VL zu modellieren. Die Operationen an diesem SFR fügen keine neuen Anforderungen hinzu, doch das SFR wurde notwendig, um die Abhängigkeiten von FCS_COP.1/AK.SigVer.BNetzA-VL zu erfüllen. Die Sicherheitsanforderung wird dem Ziel O.AK.Update zugeordnet, in Anlehnung an die SFR zur Aktualisierung der TSL.

FIA_API.1/AK.TLS
Die Sicherheitsanforderung FIA_API.1/AK.TLS wurde eingeführt, um die Anforderung GS-A_4384-01 („TLS-Verbindungen“) [gemSpec_Krypt] zu erfüllen, die fordert, dass sich der Konnektor mit einem X.509 Zertifikat identifizieren muss, wenn er Server in einer TLS-Verbindung ist. Die Sicherheitsanforderung erfüllt das Sicherheitsziel O.AK.LAN.

FIA_SOS.1/AK.CS.Passwörter

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

FCS_COP.1/AK.ECIES

Die Sicherheitsanforderung FCS_COP.1/AK.ECIES wurde eingeführt, um das ECIES-Verfahren für den Verschlüsselungsdienst abzubilden. Dieses Verfahren ist für den Konnektor der Ausbaustufe PTV 5+ gefordert, um die Migration auf das „120-Bit-Sicherheitsniveau“ zu vollziehen [gemSpec_Krypt, Abschnitt 5.7]. Das Schutzprofil [BSI-CC-PP-0098] macht keine Aussagen zu ECIES.

6.7. Erklärung für die gewählte EAL-Stufe

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

7. ASE_TSS: Basiskonnektor

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

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

Die beiden Abschnitte 7.4 und 7.5 zeigen tabellarisch die Zusammenhänge zwischen den Sicherheitsfunktionen des TOE und den Sicherheitsanforderungen, die dieses Security Target in den Abschnitten 6.2 (für den Netzkonnektor) und 6.3 (für den Anwendungskonnektor) aufstellt. Auch hier sind die NK-spezifischen Angaben aus dem Security Target des NK übernommen.

Dieses Kapitel beschreibt die Funktionalität des Basiskonnektors. Das Folgekapitel setzt ASE_TSS fort, indem die Anforderungen der Fachmodule an den TOE beschrieben werden und aufgelistet wird, wie der TOE diese Anforderungen erfüllt. Das Folgekapitel gehört somit formal zum zu prüfenden Umfang des Security Targets.

Der Produkttypsteckbrief PTV 5+ verlangt vom Hersteller eine Erklärung, dass die nicht vom Schutzprofil abgedeckten Anforderungen durch das Security Target abgedeckt sind [gemProdT_Kon_PTV5P, Abschnitt 3.2.1]. Diese Anforderungen werden im vorliegenden Kapitel explizit genannt und in die Beschreibung der Sicherheitsfunktionalität eingeflochten. Zusätzlich listet Anhang D die Anforderungen auf. Dieser Anhang ist *Teil der TOE Summary Specification* und somit vom Evaluator in die Prüfung von ASE_TSS einzubeziehen.

7.1. TOE Sicherheitsfunktionen des Netzkonnektors

7.1.1. VPN-Client (SF.VPN)

Die Sicherheitsfunktion SF.VPN erstellt sichere Kommunikationskanäle zwischen dem TOE und einem entfernten, vertrauenswürdigen IT-Produkt. Dazu wird eine IKEv2 Implementierung verwendet. Diese Kanäle sind logisch von anderen Kommunikationskanälen separiert. Sie bieten gesicherte Identifizierung der Endpunkte und Schutz der über den Kanal übertragenen Daten vor Manipulation und Preisgabe. Solche Kanäle werden vom Konnektor für Verbindungen in die Telematikinfrastruktur und zum SIS verwendet. Der TOE verwendet die Identität auf der gSMC-K#1, um sich gegnüber den entfernten VPN-Konzentratoren zu authentisieren.

Umgesetzte SFR	
FTP_ITC.1/NK.VPN_SIS	FTP_ITC.1/NK.VPN_TI

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 nicht-wohlgeformeten Pakete werden verworfen.

Der TOE führt Buch über den Status aller seiner Netzwerkverbindungen, sowie über deren relevante Informationen. Dafür setzt der TOE den Netfilter des Linux Kernels ein.

Das Hoch- und Herunterfahren des Paketfilters wird im Audit-Log des Konnektors protokolliert. Ebenso werden Informationen protokolliert, die für Basic Intrusion Prevention benötigt werden. Vorsichtsmaßnahmen sind implementiert, um zu verhindern, dass das Audit-Log mit speziell gefertigten Nachrichten geflutet wird. So könnte ein Angreifer versuchen, wichtige Nachrichten im Log zu überschreiben.

Umgesetzte SFR
FDP_IFF.1/NK.PF

7.1.3. Netzbasierte Sicherheitsfunktionen (SF.NetworkServices)

Die Sicherheitsfunktion SF.NetworkServices stellt dem TOE zuverlässige Zeitstempel zur Verfügung. Eine Referenzzeit wird über den VPN-Kanal von einem vertrauenswürdigen NTP-Server in der Telematikinfrastruktur bezogen. Dabei wird NTP in Version 4 verwendet [RFC 5905]. Die Abweichung zwischen der Netzwerkzeit und der lokalen Zeit im TOE darf maximal 1 Stunde betragen. Der TOE verwendet die Uhrzeit hauptsächlich, um die Gültigkeit von Zertifikaten zu prüfen und um Protokolleinträge mit Zeitstempel schreiben zu können. Die Synchronisation der Zeit mit dem NTP-Server findet nach dem Boot-Vorgang kontinuierlich statt. Die Intervalle zwischen den Synchronisationsabrufen betragen zwischen 64 und 1024 Sekunden, wie im NTP-Protokoll vorgesehen.

Umgesetzte SFR
FPT_STM.1/NK

Alle Anwendungen im TOE können über SF.NetworkServices die aktuelle Zeit erfragen. Der TOE stellt die Uhrzeit auch über seinen Zeitdienst an der Schnittstelle LS.LAN zur Verfügung (ebenfalls mit NTPv4). Cliensysteme und andere Nutzer im LAN des Leistungserbringers können den Zeitdienst verwenden.

Der TOE bietet weitere Netzwerkdienste für die Clientsysteme im LAN an:

- DHCP Server für die Konfiguration von Systemen mit IP-Adressen und Netzwerkparametern
- DNS Server für die Namensauflösung

7.1.4. Selbstschutz (SF.SelfProtection/NK)

Die Sicherheitsfunktion SF.SelfProtection/NK ist dafür verantwortlich, den TOE und die Daten, die er verarbeitet, vor Angriffen und Manipulation zu schützen.

Sensible Daten werden aus dem Arbeitsspeicher gelöscht, sobald sie nicht mehr verwendet werden. Das umfasst kryptographische Schlüssel, Session Keys, kurzlebige Schlüssel während des Ver- und Entschlüsselungsvorgangs, aber auch sensible Benutzerddaten. Das Löschen wird durch aktives Überschreiben der entsprechenden Speicherbereiche mit einer Konstante oder pseudo-zufälligen Werten umgesetzt.

Umgesetzte SFR	
FCS_CKM.4/NK	FDP_RIP.1/NK

Der TOE kann eine Reihe von Selbsttests ausführen, um seine Integrität und die Funktionsfähigkeit seiner eigenen Sicherheitsfunktionen und Komponenten zu beweisen. Abhängig von deren Ausprägung werden die Selbsttests entweder beim Systemstart, während des normalen Betriebs oder zu beiden Gelegenheiten ausgeführt. Der Administrator kann die Selbsttests ebenfalls starten. Folgende Selbsttests sind umgesetzt:

- Prüfung auf Integrität des sicheren Datenspeichers
- Prüfung auf Integrität des ausführbaren Codes der TOE Sicherheitsfunktionen.

Der sichere Datenspeicher speichert die Konfiguration des TOE in einem verschlüsselten Dateisystem. Die Integrität des sicheren Datenspeichers wird sichergestellt, indem für jede Datei des Dateisystems ein SHA-256 Hash berechnet, signiert und 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) und GS-A_4358-01 (für QES). GS-A_4358-01 nimmt Bezug auf den SOG-IS Katalog in Version 1.2 und verweist auf die dort angegebenen Laufzeiten der Algorithmen [SOG-IS 2020]. 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. Tabelle 7.2 zeigt die entsprechende Auflistung für qualifizierte elektronische Signaturen. 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].

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.

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

Algorithmus	Key Length	gematik	SOG-IS
RSASSA-PKCS1-v1_5	2048	2022	2025[†]
	>3000	–[*]	2027+[‡]
RSASSA-PSS	2048	(wie SOG-IS)	2025[†]
	>3000	(wie SOG-IS)	∞[×]
ECDSA	256	2023+	∞[×]

[*] GS-A_4358-01 macht zur Verwendung keine Aussage.
[†] *Legacy* mit Ablaufdatum wegen Schlüssellänge.
[‡] *Legacy* ohne Ablaufdatum wegen Padding
[×] *Recommended* ohne Ablaufdatum

Tabelle 7.2.: Algorithmen für die Erstellung und Prüfung qualifizierter elektronischer Signaturen

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 230. 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. TOE Sicherheitsfunktionen des Konnektors

7.2.1. Kryptografische Dienste/AK (SF.CryptographicServices/AK)

Hash-Algorithmen für den AK

Die Sicherheitsanforderung FCS_COP.1/AK.SHA fordert die Umsetzung sicherer Hash-Algorithmen. Der TOE bietet Funktionen zur Berechnung von Hashwerten nach den Algorithmen SHA-256, SHA-384 und SHA-512.

Umgesetzte SFR
FCS_COP.1/AK.SHA

AES Schlüsselerzeugung

Weiterhin setzt die Sicherheitsfunktion das Erzeugen und Zerstören kryptographischer Schlüssel um. Um ausreichend sichere AES Schlüssel zu erzeugen, wird der kartenbasierte Zufallsgenerator nach FCS_RNG.1/Hash_DRBG herangezogen. Das sichere Löschen kryptographischen Materials wird durch das Überschreiben mit festen Werten erreicht.

Umgesetzte SFR	
FCS_CKM.4/AK	FCS_CKM.1/AK.AES

Zertifikatsdienst (BNetzA-VL)

Der TOE verwendet in verschiedenen Use Cases kryptographische Zertifikate und entsprechende Validierungsverfahren, Die konkreten Schritte zur Validierung eines Zertifikats hängen von der Art des Zertifikats ab. Dabei werden CVC und X.509 Zertifikate unterschiedlich behandelt. Innerhalb der X.509 Zertifikate wird zwischen qualifizierten und nicht-qualifizierten Zertifikaten unterschieden. Bei den nicht-qualifizierten Zertifikaten wiederum macht es einen Unterschied, ob ein Zertifikat aus dem Vertrauensraum der gematik oder aus dem herstellerspezifischen Vertrauensraum der KoCo PKI stammt. Somit ergeben sich vier verschiedene Kategorien von Zertifikaten.

Der Ablauf bei der Zertifikatsprüfung entspricht dem Ablauf, wie er in Unterabschnitt 7.1.7 für den Zertifikatsdienst des Netzkonnektors in der Funktion SF.CryptographicServices/NK beschrieben ist.

Dem Zertifikatsdienst des Anwendungskonnektors fällt die Prüfung der BNetzA-VL und ihrer Signatur zu.

Umgesetzte SFR	
FPT_TDC.1/AK	FCS_COP.1/AK.SigVer.BNetzA-VL

7.2.2. TLS Protokoll (SF.TLS)

Der TOE nutzt TLS zur Kommunikation mit anderen IT-Systemen sowohl in der Telematikinfrastruktur, im Internet als auch im LAN des Leistungserbringers. Tabelle B.5 zeigt die TLS-Verbindungen der KoCoBox MED+.

Die Sicherheitsanforderungen an verschiedene Verbindungen des TOE mit anderen IT-Produkten werden durch die Sicherheitsfunktion SF.TLS umgesetzt. Bei diesen Sicherheitsanforderungen geht es primär um die logische Separation der Verbindung von anderen Kommunikationskanälen, sowie die Forderung von Integrität und Authentizität der Verbindung. Die Sicherheitsfunktion regelt auch, mit welchem Zertifikat sich der TOE gegenüber den Kommunikationspartnern authentisiert.

Umgesetzte SFR		
FDP_ACC.1/AK.TLS	FDP_ACF.1/AK.TLS	FDP_UIT.1/AK.TLS
FDP_UCT.1/AK.TLS	FTP_ITC.1/AK.VZD	FTP_ITC.1/AK.eHKT
FTP_ITC.1/AK.CS	FTP_ITC.1/AK.FD	FTP_ITC.1/AK.KSR
FTP_ITC.1/AK.TSL	FIA_API.1/AK.TLS	FDP_ITC.2/AK.BNetzA-VL

Das TLS Protokoll wird im TOE von den Java Secure Socket Extension (JSSE) implementiert, das Teil der Java-Laufzeitumgebung ist. JSSE wird durch Konfigurationsvorgaben und eigene Anpassungen so gehärtet, dass die Anforderungen des Schutzprofils umgesetzt werden. Die kryptographischen Eigenschaften der TLS Verbindungen werden durch die Sicherheitsfunktion SF.CryptographicServices/NK des Netzkonnektor festgelegt und umgesetzt.

Die AK-TLS-SFP sieht in ihrer Sicherheitsanforderung FDP_ACF.1/AK.TLS an verschiedenen Stellen einen „TLSConnectionIdentifier“ vor, auf den Bezug genommen werden muss, um eine TLS Verbindung nutzen zu können. Diese Maßnahme wird für TLS-Verbindungen innerhalb des TOEs nicht durch ein Sicherheitsattribut umgesetzt. Im TOE wird die Separation der TLS-Verbindungen durch Socket-Abstracktionen und die darauf basierenden Objektreferenzen umgesetzt, die vom Framework JSSE implementiert werden. Die Objektreferenzen sind als `private` gekennzeichnet oder lokale Variablen, sind also nur innerhalb des aktuellen Threads erreichbar.

Die Spezifikation des Konnektors sieht vor, dass über den Konfigurationswert *ANCL_DVD_OPEN* gesteuert wird, ob der Konnektor auch bei verpflichtender Nutzung von TLS gegenüber den Clientsystemen (*ANCL_TLS_MANDATORY* aktiviert) den unverschlüsselten Zugriff auf das Diensteverzeichnis unter */conector.sds* erlaubt. Dieser Konfigurationswert hat für den TOE keine Bedeutung mehr, bleibt aber aus Kompatibilitätsgründen mit den Primärsystemen erhalten.

Für das Fachmodul ePA setzt der TOE das Subjekt S_TLS_Dienst um. Der TLS-Dienst implementiert den TLSConnectionIdentifier in Form einer eindeutigen ID. Fachmodule erhalten nach Anforderung einer TLS-Verbindung diesen Identifier. Die Kenntnis dieser ID ist notwendig, um die TLS-Verbindung nutzen zu können.

7.2.3. Authentisierung (SF.Authentication)

Zusätzlich zur Authentisierung mit kryptographischen Zertifikaten ist der TOE in der Lage, Authentisierungen anhand von Passwörtern oder zuvor ausgehandelten Geheimnissen (preshared secrets) durch-

zuführen. Die Sicherheitsanforderung FIA_UAU.5/AK formuliert die Authentisierungsverfahren für Administratoren, Clientsysteme, Smart Cards und für eHealth-Kartenterminals.

Management-Schnittstelle

Für die Authentisierung von Administratoren an der Management-Schnittstelle der KoCoBox MED+ werden Passwörter verwendet, die über die Management-Schnittstelle vergeben werden. Diese Passwörter unterliegen Beschränkungen, die in FIA_SOS.1/AK.Passwörter formuliert sind. Passwörter werden im TOE verschlüsselt abgespeichert. Wenn bei der Authentisierung eine ungültige Kombination aus Benutzernamen und Passwort eingegeben wird, erzwingt der TOE eine dreisekündige Pause vor der nächsten Eingabemöglichkeit. Nach dem dritten aufeinander folgenden fehlgeschlagenen Anmeldeversuch desselben Benutzers wird der Benutzer für 60 Sekunden gesperrt. Jeder weitere Fehlversuch führt zu einer erneuten Sperre von 60 Sekunden. Diese Zwangspause erstreckt sich nicht auf eine Netzwerkverbindung, sondern auf den übermittelten Benutzernamen. Der TOE initiiert nach einem durch den Super-Admin konfigurierbaren Zeitraum (Voreinstellung: 120 Tage) einen Passwortwechsel beim nächsten Login. Der Zeitraum kann zwischen 30 und 365 Tagen konfiguriert werden.

Clientsysteme

Abhängig von der Konfiguration des Konnektors kann sich ein Clientsytem anhand eines X.509 Zertifikats oder anhand eines Passworts authentisieren (FMT_MSA.1/AK.TLS, FMT_MSA.3/AK.TLS). Die Regeln für die Passwörter für Clientsysteme sind in FIA_SOS.1/AK.CS.Passwörter beschrieben. Hierbei ist besonders ST-Anwendungshinweis 24 zu beachten. Zur Verhinderung von Brute-Force-Angriffen wird nach einem fehlgeschlagenen Authentisierungsversuch eine Sperre für das Clientsystem verhängt. Die Dauer der Sperre beträgt 3 Sekunden. In dieser Zeit kann sich das gesperrte Clientsystem nicht erneut authentisieren. Dadurch wird verhindert, dass ein Angreifer gleichzeitig mit mehreren Angriffen versucht, das Passwort zu erraten. Diese Maßnahme reduziert die Erfolgsaussicht eines Brute-Force-Angriffs erheblich.

Administratoren können Zertifikate für Clientsysteme entweder importieren oder vom Konnektor erzeugen lassen. Erzeugte Zertifikate werden in einem passwortgeschützten PKCS12-Container ausgeliefert.

Kartenterminals

Die Authentisierung von eHealth-Kartenterminals erfolgt in zwei Stufen: Zuerst wird das Kartenterminal im Rahmen des TLS-Handshakes anhand eines X.509 Zertifikats authentisiert, das von der SMC-KT des eHealth-Kartenterminals stammt[1]. In der zweiten Stufe wird ein Challenge-Response basiertes Verfahren verwendet. Der Konnektor sendet das Kommando EHEALTH TERMINAL AUTHENTICATE an das Kartenterminal (FIA_SOS.2/AK.PairG).

Kartenbasierte Authentisierung

Im Kontext der Smart Card basierten Operationen ist es notwendig, dass der Konnektor die gegenseitige Authentisierung von Smart Cards ermöglicht. Dieses Verfahren wird Card to Card (C2C) Authentisierung genannt. Der Konnektor unterstützt drei Varianten dieses Verfahrens: einseitige Authentisierung, gegenseitige Authentisierung und gegenseitige Authentisierung mit Ableitung eines kryptographischen Schlüssels (FIA_UAU.5/AK und FIA_API.1/AK).

Bei Stapel- oder Komfortsignaturen muss sich der TOE gegenüber der QSEE (also dem HBAx) authentisieren; dazu wird das Card2Card-Verfahren angewendet. Der Konnektor weist sich gegenüber

[1] Die Formulierung in FIA_UAU.5/AK kann missverstanden werden, dass das Pairing-Geheimnis in die Authentisierung des TLS-Kanals eingeht. Dort kommen aber ausschließlich X.509 Zertifikate zum Einsatz, vgl. ST-Anwendungshinweis 25.

dem HBAx mit der gSMC-K#3 aus. Die zur Authentisierung verwendete gSMC-K ist nicht konfigurierbar, der Ablauf der Authentisierung selbst wird von den beiden Karten bestimmt, sodass der TOE keinen Einfluss darauf hat.

Der TOE unterstützt die einseitige und gegenseitige asymmetrische Authentisierung von Chipkarten (Card2Card), die gegenseitige Authentisierung auch mit Ableitung eines symmetrischen Schlüssels und Etablierung eines sicheren Kommunikationskanals (Trusted Channel). Weiterhin unterstützt der TOE die gegenseitige symmetrische Authentisierung mit einer Chipkarte einschließlich Aushandlung symmetrischer Schlüssel für einen Secure Messaging Kanal. Die Implementierung des Card2Card Mechanismus bildet streng die Spezifikationslage ab, wie in TUC_KON_005 [gemSpec_Kon] beschrieben. Die Funktionalität wird im Rahmen unterschiedlicher UseCases genutzt, eine detaillierte Auflistung hierzu findet sich ebenfalls in TUC_KON_005.

Die Funktionalität zur Erstellung einer qualifizierten Signatur wird durch den Signaturdienst über eine definierte Schnittstelle zur Verfügung gestellt. Wird die Erstellung einer qualifizierten Signatur über diese Schnittstelle angestoßen, prüft die Anwendungslogik die relevante Konfiguration und Parametrisierung daraufhin, ob die Nutzung eines sicheren Kanals zwischen TOE (gSMC-K#3) und HBA (QSEE) notwendig ist. Wenn es sich um einen HBA als Signaturerstellungseinheit handelt und außerdem entweder das SecurityEnvironment SE_2 gesetzt ist oder es sich um eine Stapel- oder Komfortsignatur handelt, wird der Aufbau des sicheren Kanals (C2C MUTUAL+TC) angestoßen.

Nur wenn der Kanal sicher aufgebaut werden konnte, wird die Signaturerstellung fortgesetzt. Kommt es zu Fehlern beim Aufbau des sicheren Kanals, wird die Signaturerstellung abgebrochen und eine Exception erzeugt, die im weiteren Workflow in einen SOAPFault umgewandelt wird.

In einem CV-Zertifikat einer Chipkarte ist das Zugriffsprofil dieser Chipkarte enthalten. Bei der gegenseitigen Authentisierung von Chipkarten wird dieses Zugriffsprofil ausgewertet.

Die KoCoBox MED+ führt beim Systemstart automatisierte Prozesse durch, bspw. den Selbsttest. Dies erfordert, dass bestimmte Aktionen bereits zugelassen sind, bevor ein Benutzer authentisiert ist. Solche Aktionen werden zu einem späteren Zeitpunkt wieder eingeschränkt (FIA_UID.1/AK, FIA_UAU.1/AK).

Umgesetzte SFR		
FIA_UAU.1/AK	FIA_UID.1/AK	FIA_SOS.2/AK.PairG
FIA_UAU.5/AK	FIA_API.1/AK	FIA_SOS.1/AK.Passwörter
FMT_MSA.1/AK.TLS	FMT_MSA.3/AK.TLS	FIA_SOS.1/AK.CS.Passwörter
FTP_ITC.1/AK.QSEE		

7.2.4. Zugriffssteuerung (SF.AccessControl)

Eingehende Requests von Clientsytemen werden vom TOE anhand eines Regelwerks zugelassen oder abgelehnt. Die Datengrundlage für dieses Regelwerk ist das Informationsmodell des Konnektors. Ein eingehender Request enthält die IDs des Mandanten, des Clientsystems und des Arbeitsplatzes, von dem aus der Request generiert wurde. Diese Angaben bilden den Kontext des Requests. Das Informationsmodell definiert die Ressourcen, die vom Konnektor verwaltet werden. Es enthält transiente und persistente Objekte, aber auch Beschreibungen der Relationen zwischen dieses Objekten. Das Regelwerk, das auf Basis der Daten des Informationsmodells die Zugriffe erlaubt, nutzt die Daten des Kontexts des Requests als Eingangsdaten für die Regeln (FDP_ACC.1/AK.Infomod und FDP_ACF.1/AK.Infomod).

Die transienten Objekte des Informationsmodells werden erzeugt, wenn dem Konnektor Ressourcen zugeordnet werden. Solche Objekte werden automatisch wieder gelöscht, wenn die Ressourcen entfernt werden. Die persistenten Objekte des Informationsmodells hingegen werden von einem Benutzer mit der Rolle Administrator verwaltet (FMT_MSA.1/AK.Infomod). Default-Werte (Standardvorgaben) existieren im Informationsmodell des Konnektors nicht. Somit kann ein Administrator auch keine abweichenden Default-Werte spezifizieren (FMT_MSA.3/AK.Infomod).

Die Sicherheitsfunktionalität SF.AccessControl setzt den TUC_KON_000 („Prüfe Zugriffsberechtigung“) um.

Umgesetzte SFR	
FDP_ACC.1/AK.Infomod	FDP_ACF.1/AK.Infomod
FMT_MSA.1/AK.Infomod	FMT_MSA.3/AK.Infomod

7.2.5. Management der eHealth-Kartenterminals (SF.CardTerminalMgmt)

Der Kartenterminaldienst des TOE folgt den Spezifikationen der gematik in [gemSpec_Kon]. Seine Aufgabe ist es, die Kartenterminals und die Verbindungen zu den Kartenterminals zu managen. Ein dem Konnektor bekanntes Kartenterminal befindet sich aus Sicht des Konnektors ein einem von vier Zuständen: *bekannt*, *zugewiesen*, *gepairt* und *aktiv*. Im Zustand *aktiv* gibt es zwei Varianten: Das Kartenterminal ist entweder *verbunden* oder nicht. Ein Kartenterminal kann vom Konnektor nur in TUCs verwendet werden, wenn es im Zustand *aktiv/verbunden* ist.

Den Clientsystemen und internen Benutzern stellt der Kartenterminaldienst Funktionen zur Interaktion mit dem Kartenterminal zur Verfügung:

- Anfordern einer Karte
- Auswerfen einer Karte

Dies sind die einzig möglichen Interaktionen von außen. Interne Benutzer können darüber hinaus eine weitere Funktion nutzen:

- Darstellen von Texten auf dem Display des Kartenterminals

Die Funktionalitäten des Kartenterminaldienstes und des Kartendienstes (zur Kommunikation mit den Karten selbst, in Abgrenzung zur Kommunikation mit den Kartenterminals) bilden ein gemeinsames logisches Subsystem. Ausschließlich dieses Subsystem sendet APDUs an Karten oder Kartenterminals, wodurch die Vorgaben der Anforderungen FDP_ACC.1/AK.eHKT und FDP_ACF.1/AK.eHKT umgesetzt werden.

Die Kommunikation mit den Kartenterminals erfordert stets eine gegenseitig authentisierte TLS-Verbindung, die gemäß den Sicherheitsattributen in SF.TLS konfiguriert ist (FDP_UCT.1/AK.TLS, FDP_UIT.1/AK.TLS, FTP_ITC.1/AK.eHKT und FPT_TEE.1/AK).

Diejenigen Attribute der Kartenterminals, die dem TOE bekannt sind, stellen einen Teil der Konfigurationsdaten des Konnektors dar und können folglich nur von einem Benutzer mit der Rolle Administrator administriert und exportiert werden (FMT_MTD.1/AK.eHKT_Abf, FMT_MTD.1/AK.eHKT_Mod).

Ein Kartenterminal ist im Konnektor unter seinem SICCT-Terminalnamen bekannt. Der Name wird in der Spezifikation auch als *FriendlyName* bezeichnet. Für den *FriendlyName* gelten Einschränkungen in Bezug auf die Länge und den Zeichensatz: Er darf zwischen 1 und 32 Zeichen lang sein und Zeichen aus

der Menge a–z, A–Z, 0–9 sowie den Bindestrich „–“ enthalten. Kartenterminals, die bei einem Unicast gefunden werden und deren Name nicht diesen Vorgaben entspricht, werden nicht angezeigt und können nicht gepairt werden. Wenn bestehende Kartenterminals ungültige Zeichen im Namen haben, werden diese Kartenterminals nach Aktualisierung gelöscht und anschließend über den *CT/ERROR 20080* im Sicherheitsprotokoll protokolliert.

Umgesetzte SFR		
FDP_ACC.1/AK.eHKT	FDP_ACF.1/AK.eHKT	FTP_ITC.1/AK.eHKT
FDP_UCT.1/AK.TLS	FDP_UIT.1/AK.TLS	FPT_TEE.1/AK
FMT_MTD.1/AK.eHKT_Abf	FMT_MTD.1/AK.eHKT_Mod	

7.2.6. Management der Smart Cards (SF.SmartCardMgmt)

Die unter SF.SmartCardMgmt zusammengefassten Sicherheitsfunktionen beschreiben die Verfahren zum Umgang des Konnektors mit Smart Cards der Typen HBA, SMC-B, eGK und KVK, die in ein vom Konnektor kontrolliertes e-Health Kartenterminal eingesteckt werden.

Wenn eine Smart Card in ein solches Kartenterminal eingesteckt wird, werden Typ und Version der Karte identifiziert. Wenn die Karte keinem der bekannten Typen entspricht, wird sie als *unbekannt* markiert und kann nicht für weitere Operationen verwendet werden. Gehört die Karte zu einem der bekannten Typen, erstellt der Kartendienst ein Objekt für diese Karte und weist diesem ein Kartenhandle zu, sodass die Karte referenziert werden kann. Das Kartenhandle ist solange gültig, bis die Karte aus dem Kartenterminal herausgezogen wird. Andere Dienste des Konnektors können die Karte verwenden. Externen Entitäten wie Clientsytemen und Fachdiensten dürfen die Karte nur eingeschränkt verwenden. „Verwenden“ bedeutet hier, dass die Karte über den Kartendienst referenziert werden kann. Der direkte Zugriff auf die Karte und das Versenden von Kartenkommandos ist dem Kartendienst vorbehalten, vgl. Unterabschnitt 7.2.5.

Kartenbasierte Operationen werden im Kontext von Kartensitzungen (card session) ausgeführt. Diese Kartensitzungen werden vom Konnektor kontrolliert und laufen isoliert voneinander. Die Sicherheitszustände der Karten sind an Kartensitzungen gekoppelt und somit streng separiert. Der Sicherheitszustand einer Kartensitzung kann durch Interaktion mit dem Benutzer (durch Eingabe einer PIN) oder durch Card-to-Card-Authentisierung verändert werden.

Bei einer PIN-Authentisierung gibt der Benutzer seine PIN am Kartenterminal ein, in dem Karte steckt. Es ist auch möglich, die PIN an einem entfernten Kartenterminal einzugeben, wenn dieses entsprechend konfiguriert ist. In diesem Fall sorgt der Konnektor für den Aufbau eines sicheren Kanals (secure messaging channel), der durch das kryptographische Material der beteiligten Karten abgesichert wird.

Bei einer Card-to-card-Authentisierung steuert der Konnektor den Prozess, in dem eine Smart Card sich gegenüber einer anderen Karte im Rahmen eines challenge-response Verfahrens authentisiert. Auch hier wird kryptographisches Material verwendet, das sicher auf den Karten abgelegt sind – in diesem Fall die card verification certificates (CVC).

Die privaten Schlüssel der vom Konnektor kontrollierten Smart Cards werden für digitale Signaturen und Entschlüsselung verwendet. Darüber hinaus bieten die Karten noch begrenzten Speicherplatz für Benutzerdaten.

Die vorliegende Implementierung weicht architekturell von den Subjekten ab, die im Schutzprofil definiert werden. Die Sicherheitsanforderung FDP_ACF.1.2/AK.KD macht präzise Aussagen, welche Teile des TOE welche Aufgaben in Bezug auf Chipkarten haben. Die KoCoBox MED+ ist so aufgebaut,

dass *ausschließlich* der Kartendienst Chipkartenkommandos an die Karte absetzt. In Abgrenzung dazu kommunizieren weder der Verschlüsselungs- noch der Signaturdienst mit der Karte. Dies ist zu berücksichtigen, wenn die Architektur bewertet wird.

Umgesetzte SFR		
FDP_ACC.1/AK.KD	FDP_ACC.1/AK.PIN	FPT_TEE.1/AK
FDP_ACF.1/AK.KD	FDP_ACF.1/AK.PIN	FMT_MSA.4/AK
FMT_MTD.1/AK.Zert		

7.2.7. Signaturdienst (SF.SignatureService)

Der TOE enthält eine Signaturerstellungs- und Verifikationsanwendung (SCaVA). Diese Funktionen werden vom Signaturdienst bereitgestellt und stehen internen Benutzern und den Clientsytemen zur Verfügung. Die SCaVA kann sowohl qualifizierte als auch nicht-qualifizierte elektronische Signaturen erstellen und verifizieren. Die unterstützten Dateiformate sind:

Für nonQES XML (nur für Fachmodule), PDF/A, Text, TIFF und Binärdaten

Für QES XML, PDF/A, Text, TIFF

Die Konnektorspezifikation definiert in den übergreifenden Festlegungen die Begriffe *nonQES_DocFormate* und *QES_DocFormate* um die Dateiformate zu referenzieren. Der Signaturdienst des TOE unterstützt bei der Verifkation von Signaturen verschiedene Verfahren:

- PKCS#1 RSASSA-PSS
- PKCS#1 RSASSA-PKCS1-v1_5
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Die Sicherheitsfunktion SF.SignatureService erfüllt die Anforderungen, die durch die SFR aus der Familie FCS_COP aufgestellt werden.

Umgesetzte SFR		
FCS_COP.1/AK.XML.Sign	FCS_COP.1/AK.CMS.Sign	FCS_COP.1/AK.PDF.Sign
FCS_COP.1/AK.XML.SigPr	FCS_COP.1/AK.CMS.SigPr	FCS_COP.1/AK.PDF.SigPr
FCS_COP.1/AK.SigVer.SSA	FCS_COP.1/AK.SigVer.PSS	FCS_COP.1/AK.SigVer.ECDSA

Der TOE unterstützt bei der Erstellung von Signaturen auf CMS, PDF und XML-Dokumenten die Verfahren RSASSA-PSS oder ECDSA und verwendet *signPSS* oder *signECDSA* als *AlgorithmIdentifier*. [2] Das Signaturverfahren wird durch Angabe des optionalen Parameters *crypt* beim Aufruf der Operation *SignDocument* ausgewählt. Per Default ist das Verfahren RSASSA-PSS voreingestellt.

Die Nutzung des Signaturdienstes wird durch SFR gesteuert, die in den Signaturerstellung-SFP und Signature Verification-SFP des Schutzprofils definiert werden. Nicht nur die Nutzung des Signaturdienstes, sondern auch die inneren Abläufe unterliegen den SFR.

[2] Das Verfahren PKCS#1 RSASSA-PKCS1-v1_5 wird nur für das Signieren von Binärstrings (bei der Operation *External Authenticate*) verwendet.

Umgesetzte SFR		
FDP_ACC.1/AK.Sgen	FDP_ACC.1/AK.SigPr	FDP_ITC.2/AK.Sig
FDP_ACF.1/AK.Sgen	FDP_ACF.1/AK.SigPr	FMT_MSA.3/AK.Sig

Signaturen werden von den beteiligten Smart Cards erzeugt, die unter der Kontrolle des Kartendienstes stehen. Der Signaturdienst verhält sich unterschiedlich, je nachdem ob qualifizierte oder nichtqualifizierte Signaturen verarbeitet werden sollen. Wenn ein Dokumentenstapel mit einer qualifizierten Signatur versehen wird, sind besondere Maßnahmen erforderlich. FIA_UAU.5.2/AK(4) fordert, dass die TSF den HBA authentisieren:

Als QSEE wird der HBA authentisiert, wenn beim Stecken der Karte der richtige Typ gemäß [gemSpec_COS] und [gemSpec_HBA_ObjSys] vorhanden ist. Das CardHandle wird als Merkmal verwendet, um die Karte später zu identifizieren und mit einem Signatur-Request zu assoziieren.

Als Empfänger der DTBS und der PIN wird der HBA authentisiert, wenn beim Card2Card Schlüssel ausgehandelt werden.

Fortlaufend während des Signaturprozesses wird der HBA authentisiert durch den Aufbau eines Trusted Channel zwischen der gSMC-K#3 und dem HBA.

Umgesetzte SFR	
FTP_ITC.1/AK.QSEE	FIA_UAU.5/AK

Wenn eine qualifizierte Signatur erstellt wird, wird der Benutzer durch die Eingabe der PIN.QES der HBAx Smart Card authentisiert. Diese Eingabe kann entweder an dem lokalen Kartenterminal erfolgen, in dem auch der HBAx gesteckt ist, oder aber an einem entfernten Kartenterminal (über das Remote PIN Verfahren). In diesem Fall steckt der HBAx in einem zentralen Kartenterminal, das nicht am Arbeitsplatz des Benutzers steht. Der Benutzer gibt die PIN am Kartenterminal seines Arbeitsplatzes ein (das als remote Kartenterminal konfiguriert sein muss). Es besteht eine sichere Verbindung (secure messaging) zwischen dem Kartenterminal am Arbeitsplatz und dem Kartenterminal, das den HBAx enthält. Der Benutzer kann anhand der Jobnummer, die auf dem Display des Kartenterminals an seinem Arbeitsplatz angezeigt wird, feststellen, ob die PIN für den von ihm initiierten Signaturvorgang abgefragt wird.

Umgesetzte SFR	
FTA_TAB.1/AK.Jobnummer	FMT_MSA.4/AK
FIA_SOS.2/AK.Jobnummer	FTA_TAB.1/AK.SP

Der Benutzer des TOE soll der Authentizität der Signaturen (für QES und nonQES) und Zertifikate versichert sein. Die Sicherheitsfunktion SF.SignatureService stellt die Nachweise bereit, um diese Versicherung zu gewährleisten. Diese Nachweise stehen in Form von Verification Reports zur Verfügung, wie sie von der Konnektorspezifikation in TAB_KON_066 gefordert und profiliert werden [gemSpec_Kon, Abschnitt 4.1.8.5.2].

Dokumente und zu signierende Daten (DTBS) werden niemals permanent im TOE gespeichert, sodass eine Überwachung der DTBS zur Sicherstellung der Integrität in der vorliegenden Architektur nicht umgesetzt ist. Die Integrität der zu signierenden Daten, die von FDP_SDI.2/AK gefordert wird, setzt der TOE um, indem die von der Karte berechnete Signatur gegen den Hashwert der zu signierenden Daten geprüft wird.

Umgesetzte SFR	
FDP_DAU.2/AK.Cert	FDP_SDI.2/AK

Signaturrichtlinien

Eine besondere Bedeutung kommt im Kontext des Signaturdienstes den *Signaturrichtlinien* zu. Diese Richtlinien profilieren das Signieren von Dokumenten und das Verifizieren von Signaturen. Leider ist der Begriff „Signaturrichtlinie“ im Kontext des Konnektors nicht eindeutig gefasst. Schutzprofil und Konnektorspezifikation interpretieren den Begriff unterschiedlich. Im Folgenden werden die Interpretationen beschrieben und die für dieses Dokument angenommene Interpretation dargelegt.

Schutzprofil Das Schutzprofil interpretiert „Signaturrichtlinie“ bewusst weit. Im Glossar in [BSI-CC-PP-0098] wird der Begriff als „Profilierung der Signaturformate“ definiert. Er dient z. B. zur Unterscheidung zwischen qualifizierten und nicht-qualifizierten Signaturen. FDP_DAU.2.1/AK.QES und FDP_DAU.2.1/AK.Sig listen die vom Konnektor zu unterstützenden Dokumentformate, Signaturformate und Signaturvarianten auf; sie machen jedoch keine Aussagen darüber, welche Elemente technisch und fachlich sinnvoll verknüpfbar sind.

Darüber hinaus führt das Glossar noch die *zulässige Signaturrichtlinie* auf, die u. a. auf die Anwendbarkeit der zu signierenden Daten durch den EVG abstellt. Dies kann als Einschränkung der Kombinationsmöglichkeiten aus FDP_DAU.2.1/AK.QES verstanden werden. Gestützt wird diese Annahme durch die Anforderung aus FMT_MSA.1.1/AK.User(2)[3], die die Auswahl der Signaturrichtlinie den Benutzern des Clientsystems vorbehält.

Konnektorspezifikation Die Konnektorspezifikation interpretiert „Signaturrichtlinie“ enger als das Schutzprofil. Signaturrichtlinien im Sinne der Spezifikation profilieren die Signaturerstellung und -prüfung. Sie werden über eine URI referenziert. Der Konnektor selbst stellt keine Signaturrichtlinie zur Verfügung, es obliegt den Fachmodulen, eigene Richtlinien zu definieren [gemSpec_Kon, Abschnitt 4.1.8.1.2]. Das ist das Vorgehen im Fachmodul NFDM. Legt man diese Interpretation zugrunde, so gibt es in PTV 5+ genau eine Signaturrichtlinie.

Für dieses Security Target ist es nicht zweckdienlich, sich ausschließlich einer der beiden Interpretationen zu verschreiben und die andere nicht zu beachten. Stattdessen wird in diesem Security Target eine Interpretation angenommen, die der Obermenge der Interpretationen des Schutzprofils und der Konnektorspezifikation entspricht: Wir nehmen die Auflistungen der Elemente aus FDP_DAU.2.1/AK.QES und FDP_DAU.2.1/AK.Sig an, beschränken jedoch die Kombinierbarkeit anhand der in TAB_KON_778 vorgegebenen Einsatzbereiche. Tabelle 7.3 zeigt die verschiedenen Signaturverfahren in Bezug auf die Signatureigenschaften Gegensignatur, Parallelsignatur und OCSP-Einbettung. Zusätzlich gelten Einschränkungen bei der Verwendung von Signaturverfahren:

XAdES / QES Der Konnektor unterstützt qualifizierte Signaturen auf XML-Dokumenten ausschließlich in Verbindung mit einer benannten Signaturrichtlinie. In PTV 5+ wird die in der Firmware des TOE verankerte Signaturrichtlinie des Fachmodul NFDM [gemRL_QES_NFDM, Abschnitt 3.] berücksichtigt, andere Signaturrichtlinien für QES werden nicht akzeptiert. Mit dieser Einschränkung setzt das Security Target die Anforderung aus TIP1-A_5538 um.

[3] Allerdings gilt diese Annahme nur, wenn man die Begriffe „*zulässige* Signaturrichtlinie“ (aus dem Glossar) und „*gültige* Signaturrichtlinie“ (aus dem SFR) synonym betrachtet (Hervorhebungen in den Zitaten durch den ST-Autor). Das Schutzprofil bleibt hier vage.

Die möglichen Transformationen bei der Erzeugung und Verifikation von XAdES Signaturen wurden stark eingeschränkt. Die einzig erlaubte Transformation ist `http://www.w3.org/2006/12/xml-c14n11` (ohne Kommentare) zur Kanonisierung der XML-Daten. Durch die Beschränkung auf *Detached* Signaturen sind keine Transformationen zum Ausschneiden der Signatur notwendig.

XAdES / nonQES Der Konnektor unterstützt die Erstellung von nicht-qualifizierten Signaturen auf XML-Dokumenten im Rahmen des TUC_KON_160. Die Funktionalität wird dabei ausschließlich an der internen Schnittstelle für Fachmodule angeboten. Damit wird A_20478 umgesetzt.

PAdES PAdES Signaturen, die nicht das gesamte Dokument umfassen, werden als ungültig gewertet. Weiterhin werden keine Updates auf einem bereits signierten Dokument unterstützt:

- Es können keine OCSP-Responses in den Document Security Store eingebettet werden.
- Dokumentinkludierende Gegensignaturen in Form von PDF Serial Signatures werden nicht unterstützt.

Herstellerspezifische Signaturrichtlinien Fast alle ursprünglich vom Hersteller ergänzten Signaturrichtlinien sind inzwischen durch die Spezifikationen der gematik oder das Protection Profile vorgegeben. Folgende Vorgaben/Anpassungen können darüber hinaus als herstellerspezifische Signaturrichtlinien angesehen werden:

- Sichere Ermittlung des signierten Bereichs von PDF-Signaturen nach dem Algorithmus gemäß Vulnerability Report der Ruhr-Universität Bochum. Hierdurch wird eine Härtung gegen Universal Signature Forgery (USF), Incremental Saving Attack (ISA) und Signature Wrapping Attack (SWA) erreicht.
- Härtung der zur Erstellung und Prüfung von XML-Signaturen verwendeten XML-Schemas gegen Signature Wrapping Angriffe gemäß Empfehlungen in [RUB-XML].
- Härtung der XML-Verarbeitung (Schnittstellen und Parser) gemäß *OWASP*.
- Verbot mehrerer identischer ID-Attribute in einem XML-Dokument. Die Signaturerstellung und -prüfung muss mit einer Fehlermeldung abgebrochen werden, wenn ID-Attribute nicht eindeutig sind.
- Die Spezifikation des Konnektors stellt in A_22673 und A_22923 Anforderungen an die Verarbeitung von XML-Dokumenten und -Dateien. Der TOE setzt diese Anforderungen, insbesondere die Restriktionen aus TAB_KON_889 um. Dies gilt für alle XML-Verarbeitungen, nicht nur für SF.SignatureService

Folgt man dieser Interpretation, ist auch FMT_MSA.1/AK.User umzusetzen. Damit obliegt es der Verantwortung des Benutzers des Clientsystems, über eine entsprechende Auswahl im Clientsystem die für den speziellen Anwendungszweck angemessene Signaturrichtlinie auszuwählen.

Umgesetzte SFR		
FDP_DAU.2/AK.Sig	FDP_DAU.2/AK.QES	FMT_MSA.1/AK.User

		Parallelsignatur		Gegensignatur		OCSP-Einb.		Anz. Signat.
		Erstellen	Prüfen	Erstellen	Prüfen	Erstellen	Prüfen	
nonQES	CAdES*	✓	✓	✓	✓	✓[1]	✓[2]	unbeg.
	PAdES†	.	.	.	.	.	.	1
	XAdES×	.	.	.	.	✓	.	1
QES	CAdES*	✓	✓	✓	✓	✓	✓	unbeg.
	PAdES†	.	.	.	.	.	.	1
	XAdES‡	.	.	.	.	✓	✓	1

* Für Detached und Enveloping Signaturen
† Speichern der Signatur als Incremental Update
× Für Enveloped Signaturen von SAML2-Assertions bei Aufruf durch Fachmodule
‡ Für Detached Signaturen bei NFDM

[1] Nur bei der Erstellung von Gegensignaturen
[2] Nur bei der Prüfung von Parallelsignaturen bei der Erstellung von Gegensignaturen

Tabelle 7.3.: Signaturvarianten

External Authenticate

Der Konnektor bietet an der Außenschnittstelle die Operation *ExternalAuthenticate* an. Diese Operation signiert einen max. 512 Byte langen Binärstring, den das Clientsystem bereitstellt. Der Konnektor verwendet ausschließlich die SMC-B oder den HBA, um Signaturen für diese Operation zu erzeugen. Der Umfang der Schnittstelle ist in TIP1-A_5439 der Konnektorspezifikation definiert [gemSpec_Kon, Abschnitt 4.1.13.4.1]. Der TOE unterstützt an dieser Schnittstelle das im Schutzprofil geforderte Verfahren PKCS#1 (RSASSA-PKCS1-v1_5, RSASSA-PSS).

Umgesetzte SFR
FDP_ACF.1.2/AK.Sgen(6)

Komfortsignatur

Der Konnektor implementiert das Funktionsmerkmal *Komfortsignatur*, das es dem Benutzer ermöglicht, mehrere Stapelsignaturvorgänge ohne erneute PIN-Eingabe auszulösen [gemSpec_Kon]. Die Funktionalität muss für jeden HBA einzeln aktiviert werden.

Im Ursprungszustand ist der globale Konfigurationswert *SAK_COMFORT_SIGNATURE* auf *Disabled* gesetzt. Ein Administrator muss den Wert auf *Enabled* setzen, damit der Konnektor das Funktionsmerkmal Komfortsignatur überhaupt anbietet (TIP1-A_4680-03). Die Voraussetzung dafür ist, dass die Verbindungen zu den Clientsystemen verschlüsselt ist (*ANCL_TLS_MANDATORY = Enabled*) und dass sich Clientsysteme am Konnektor authentisieren (*ANCL_CAUT_MANDATORY = Enabled*), ebenfalls gemäß TIP1-A_4680-03. Die Aktivierung des Funktionsmerkmals Komfortsignatur über die Management-Schnittstelle ist eine globale Einstellung des TOE, die mandantenübergreifend wirksam wird; es ist nicht möglich, das Funktionsmerkmal Komfortsignatur über diese Einstellung für einzelne Mandanten zu aktivieren.

Umgesetzte SFR	
für TIP1-A_4680-03:	FMT_MSA.3/AK.Sig
	FDP_ACF.1/AK.TLS

Nur wenn *SAK_COMFORT_SIGNATURE = Enabled* ist, kann über die Operation *ActivateComfortSignature* die Funktion für einen bestimmten HBA aktiviert werden. Pro HBA können bis zu drei parallele Komfortsignatur-Sessions mit unterschiedlicher ClientSystem ID oder User ID aktiviert oder deaktiviert werden (gemäß A_22344). Beim Aktivieren der Komfortsignatur muss das Clientsystem eine User ID übergeben, die dann zukünftig für alle Signaturvorgänge präsentiert werden muss. Diese User ID identifiziert den Benutzer zusätzlich zu den üblichen Merkmalen des Aufrufkontexts.[4] Sie stellt ein Sicherheitsmerkmal dar, weswegen der TOE bei der ersten Übergabe gemäß A_20073-01 prüft, ob die User ID im Format einer UUID vorliegt [RFC 4122]. Der Konnektor akzeptiert ausschließlich User IDs der Länge 128 Bit. Der Konnektor prüft die User ID auf Eindeutigkeit gegen eine Liste der letzten 1.000 registrierten IDs (A_20074). Wenn die User ID in dieser Liste vorkommt, lehnt der TOE die Aktivierung ab. Die User ID ist ein *persönliches* Datum und als solches vom TOE geheim zu halten. Sie darf nicht protokolliert oder an einer Außenschnittstelle exponiert werden. Dies wird durch den Anwendungshinweis 203 des Schutzprofils [BSI-CC-PP-0098] zu FAU_GEN.1/AK subsumiert.

Es liegt in der Verantwortung des Clientsystems, eine ausreichend sichere User ID zu generieren. Aus Sicht des Konnektors ist dies eine Anforderung an die Umgebung.

Die so aktivierte Komfortsignatur ist immer nur für eine bestimmte Anzahl von Signaturvorgängen oder für eine bestimmte Zeit erlaubt. Die Konfigurationswerte *SAK_COMFORT_SIGNATURE_MAX* und *SAK_COMFORT_SIGNATURE_TIMER* spiegeln diese Werte wider. Beim Erreichen des einen oder des anderen Maximalwerts deaktiviert der Konnektor die Komfortsignatur für die jeweilige Session des HBA (A_19100-01, A_22352 für die Anzahl und A_18686-01, A_22459 für den Zeitpunkt). Für beide Konfigurationswerte gibt es Standardwerte, die der Administrator überschreiben kann. Die Komfortsignatur ist immer eine Stapelsignatur, sodass Secure Messaging zwischen dem Konnektor und der Signaturerstellungseinheit durchgesetzt wird. Dieser Secure Messaging-Kanal wird gemäß A_19258 über die gSMC-K#3 zum HBA mittels C.SAK.AUTD_CVC aufgebaut.

Umgesetzte SFR	
für A_20073-01:	FIA_UAU.5/AK
für A_20074:	FIA_UAU.5/AK
für A_19100-01:	FDP_ACF.1.2/AK.Sgen(4) (h),(i)
für A_19101:	FIA_UAU.5/AK (ST-Anwendungshinweis 27)
für A_18686-01:	FDP_ACF.1.2/AK.Sgen(4) (h),(i)
für TIP1-A_4680-03:	FMT_MSA.3/AK.Sig
für A_19258:	FTP_ITC.1.3/AK.QSEE

Beim Auslösen einer Komfortsignatur übergibt das Clientsystem zusätzlich zum Aufrufkontext die User ID. Der Konnektor prüft, dass genau nur der Nutzer, der den Komfortsignatur-Modus aktiviert hat (und dabei seine PIN.QES eingebeben hat) auch die Komfortsignatur für diesen HBA auslösen darf (TIP1-A_4524-03).

[4] Zwar nennt die Spezifikation dieses Sicherheitsmerkmal „User ID“, doch aus softwaretechnischer Sicht ist es einfacher, sich dieses Merkmal als eine Session ID vorzustellen.

Umgesetzte SFR	
für TIP1-A_4524-03:	FDP_ACF.1/AK.Infomod

Durch das Zurücksetzen des HBA bei *DeactivateComfortSignature* (A_19105, Schritt 5a) und beim Setzen des Parameters *SAK_COMFORT_SIGNATURE* auf *Disabled* (A_19105, zusätzlich Schritt 2) wird der Komfortsignatur-Modus deaktiviert.

Umgesetzte SFR	
für A_19105:	FDP_ACF.1.2/AK.Sgen(4) (h),(i)

7.2.8. Verschlüsselungsdienst (SF.EncryptionService)

Der Konnektor ver- und entschlüsselt über seinen Verschlüsselungsdienst Daten hybrid und symmetrisch. Gemäß Spezifikation unterstützt der TOE „Alle_DocFormate“, also die Datenformate XML, PDF/A, Text, Tiff sowie Binärdaten [vgl. gemSpec_Kon, Abschnitt 3.1.1]. Dabei kommt in der Regel das CMS-Verfahren gemäß RFC 5652 [RFC 5652] zum Einsatz. Darüber hinaus können XML Dokumente nach der W3C Recommendation „XML Encryption Syntax and Processing“ [XMLEnc] ver- und entschlüsselt werden. Das von der Spezifikation optional erlaubte S/MIME-Verfahren unterstützt der TOE nicht.

Umgesetzte SFR	
FCS_COP.1/AK.CMS.Ver	FCS_COP.1/AK.CMS.Ent
FCS_COP.1/AK.XML.Ver	FCS_COP.1/AK.XML.Ent

Die Verwendung der Sicherheitsfunktion unterliegt Regeln, die in weiteren Anforderungen formuliert sind. Dort ist auch beschrieben, wie der TOE mit den zu verschlüsselnden und den verschlüsselten Daten umzugehen hat.

Umgesetzte SFR	
FDP_ACC.1/AK.Enc	FDP_ACF.1/AK.Enc
FDP_ITC.2/AK.Enc	FDP_ETC.2/AK.Enc

7.2.8.1. Hybride Verschlüsselung

Der TOE setzt die hybride Ver- und Entschlüsselung wird gemäß der Vorgaben aus TUC_KON_070, bzw. TUC_KON_071 um. Der *symmetrische* Teil der Verschlüsselung folgt AES/GCM mit Schlüsseln der Länge 256 Bit. Dies ist der Regelfall. Ausschließlich für die Entschlüsselung von Bestandsdokumenten akzeptiert der TOE zusätzlich Schlüssel der Längen 128 Bit und 192 Bit. Der *asymmetrische* Teil unterstützt RSA-Kryptographie (2048 Bit) und ECC (256 Bit). Der Konnektor verwendet ausschließlich RSAOAEP, wie von TIP1-A_4617-02 und GS-A_4376-02 gefordert. Als Mask-Generation-Function für die Verwendung in RSAOAEP wird MGF 1 mit SHA-256 als Hash-Funktion verwendet (GS-A_4390). Das Verfahren RSA RSAES-PKCS1-v1_5 wird nicht unterstützt.

Im Fall von ECC unterstützt der TOE auch das ECIES-Verfahren, wie es in der gematik Spezifikation definiert ist [gemSpec_Krypt, Abschnitt 5.7]. Die Anforderung A_17220 definiert den Ablauf des Verfahrens grob. Ausgangspunkt für die Implementierung des TOE ist die Beschreibung des Algorithmus in der Spezifikation des COS [gemSpec_COS, Abschnitt 6.8.2.3]. Die zu verwendenden

kryptographischen Operationen sind dort präziser beschrieben. Der TOE verwendet ein zu ISO-7816 konformes Padding, wobei nur die ersten 8 Bytes verwendet werden.

Umgesetzte SFR
FCS_COP.1/AK.ECIES

7.2.8.2. Symmetrische Verschlüsselung

Bei der symmetrischen Ver- und Entschlüsselung unterscheidet die Spezifikation zwischen *Dokumenten* und *Binärdaten*. Dokumente werden mit den Abläufen in TUC_KON_072 und TUC_KON_073 ver- und entschlüsselt. Für Binärdaten sieht die Spezifikation TUC_KON_075 und TUC_KON_076 vor. Wird für die Verschlüsselung kein Schlüssel übergeben, erzeugt der TOE einen eigenen Schlüssel mit Hilfe des sicheren Zufallsgenerators, wie in FCS_CKM.1/AK.AES beschrieben.

7.2.8.3. AES/GCM

Für alle genannten Varianten verwendet der Konnektor AES/GCM als Cipher. Im Regelfall werden Schlüssel der Länge 256 Bit verwendet, Ausnahmen gelten für die Entschlüsselung von Bestandsdokumenten (s. o.). Der Initialisierungsvektor IV besteht immer aus 96 Bit zufällig erzeugter Daten. Die IVs werden grundsätzlich neu erzeugt und nicht für spätere Verwendungen gespeichert.

Umgesetzte SFR
FCS_COP.1/AK.AES

Verschlüsselungsrichtlinien

Der Verschlüsselungsdienst ist nach den Vorgaben der gematik implementiert. Korrespondierend zu den Operationen und TUCs in [gemSpec_Kon] gibt es keine expliziten oder identifizierbaren Verschlüsselungsrichtlinien. Die Vorgaben in SFRs, die auf solche Richtlinien Bezug nehmen, werden als eine Referenz auf die [gemSpec_Kon] interpretiert, um eine spezifiktionskonforme Implementierung zu gewährleisten. Der TOE verwendet die herstellereigene Verschlüsselungsrichtlinie, dass bei *XML-Verschlüsselung* ausschließlich das Gesamtdokument verschlüsselt wird. Das Ver- und Entschlüsseln von Teilbäumen wird nicht unterstützt.

Als Empfängerzertifikate werden zum Referenzzeitpunkt (Zeitpunkt der Verschlüsselung) zeitlich gültige Zertifikate mit der *KeyUsage keyEncipherment* zugelassen. Der Algorithmus der Signatur muss zum Referenzzeitpunkt zulässiggewesen sein. Weiterhin sind Zertifikate zulässig,

1. deren CA sich in der Liste der importierten CAs befindet,
2. deren CA in der TSL aktiv ist, das ENC-Zertifikat zum Referenzzeitpunkt nicht widerrufen war und die mindestens eine der folgenden Policies enthalten:
   a) OID_EGK_ENC (1.2.276.0.76.4.68)
   b) OID_EGK_ENCV (1.2.276.0.76.4.69)
   c) OID_HBA_ENC (1.2.276.0.76.4.74)
   d) OID_SMCB_ENC (1.2.276.0.76.4.202)
   e) OID_FD_ENC (1.2.276.0.76.4.76)

f) OID_VK_PT_ENC (1.2.276.0.76.4.62)

g) OID_VK_EAA_ENC (1.3.6.1.4.1.24796.1.10)

Dem Betreiber des TOE bleibt es unbenommen, CAs für Zertifikate, die den Anforderungen aus (2) nicht (mehr) genügen in die unter (1) genannte Liste einzutragen um die strikten Prüfungen unter (2) zu vermeiden.

7.2.9. Sicherer Speicher (SF.SecureStorage)

Der Konnektor verfügt über einen sicheren internen Datenspeicher, um Daten verschlüsselt und signiert abzulegen. Die Verschlüsselung ist symmetrisch und für den Benutzer transparent. Der symmetrische Schlüssel für diese Daten liegt im Netzkonnektor und ist nicht von außen manipulierbar. Jede Datei, die im sicheren Datenspeicher abgelegt ist, wird einzeln signiert. Beim Lesezugriff auf diese Datei wird die Signatur geprüft. Eine invalide Signatur versetzt den TOE in einen kritischen Betriebszustand, der den Funktionsumfang des Konnektors stark einschränkt.

Umgesetzte SFR	
FDP_ACC.1/AK.SDS	FDP_ACF.1/AK.SDS

Die kryptographischen Funktionen des sicheren Datenspeichers werden von der Sicherheitsfunktion SF.CryptographicServices/NK umgesetzt, vgl. Unterabschnitt 7.1.7, Unterabschnitt „AES / Sicherer Datenspeicher“.

7.2.10. Versichertenstammdatenmanagement (SF.VSDM)

Das Fachmodul VSDM des Konnektors liest die Versichertenstammdaten (VSD) von den elektronischen Gesundheitskarte des Patienten ein und übermittelt sie an das Praxisverwaltungssystem. Darüber hinaus können die Stammdaten auf der eGK aktualisiert werden: Der Konnektor prüft auf dem Update Flag Service der Telematikinfrastruktur, ob eine Aktualisierung für die Daten vorliegt. Ist das der Fall, vermittelt der Konnektor einen sicheren Kanal zwischen dem Versichertenstammdatendienst der TI (VSDD) und der eGK des Patienten. Wenn dieser Kanal aufgebaut ist, sind die Daten zwischen den Kommunikationspartner Ende-zu-Ende verschlüsselt. Der Konnektor leitet den verschlüsselten Datenstrom weiter, kann die Daten aber nicht selbst lesen.

Zusätzlich zur Aktualisierung der VSD kann derselbe Mechanismus verwendet werden, um das Objektsystem der eGK zu aktualisieren. Hierbei ist jedoch der Card Management Service der TI (CMS) der Kommunikationspartner der Karte, nicht der VSDD).

Der Kommunikationsablauf wird nicht von Betriebsparametern beeinflusst, die der Administrator verändern kann. Somit gibt es auch keine Standardwerte, die der Administrator mit alternativen Werten belegen kann.

Umgesetzte SFR	
FDP_ACC.1/AK.VSDM	FDP_ACF.1/AK.VSDM
FMT_MSA.3/AK.VSDM	FMT_MSA.1/AK.VSDM

7.2.11. Administration/AK (SF.Administration/AK)

Allgemeines

Der Konnektor enthält eine Management-Schnittstelle, die von einem Administrator über eine Web-Anwendung benutzt werden kann. Ein authentisierter Benutzer mit der Rolle Administrator kann die Verwaltungsoperationen vornehmen, die in [gemSpec_Kon] definiert sind. Unter anderem können so die Konfigurationsdaten der Konnektor Services angepasst werden. Jeder Service definiert seine eigene, begrenzte Menge an Konfigurationsdaten. Der Management Service selbst definiert übergreifende Konfigurationselemente.

TLS-Verbindung zur Managementschnittstelle

Die Managementschnittstelle zur Administration der KoCoBox MED+ ist in Form einer JSON-Schnittstelle umgesetzt. Die JSON-Schnittstelle ist über LS.LAN.HTTP_MGMT erreichbar. Die dafür notwendige TLS-Verbindung wird von SF.CryptographicServices/NK bereitgestellt. Diese Verbindung wird mit den Parametern in Tabelle 7.4 konfiguriert. Die TLS-Verbindung ist serverseitig durch ein Zertifikat authentisiert. Eine clientseitige Authentifizierung mit einem Zertifikat ist nicht notwendig, da sich der Administrator mit Username und Password authentifizieren muss um die Managementschnittstelle nutzen zu können (FIA_UID.1/NK.SMR, FTP_TRP.1/NK.Admin).

Die Managementschnittstelle kann von einem beliebigen Frontend bedient werden. Das Standardverfahren ist die Verwendung der Admin-Web Application, die der Konnektor bereitstellt. Die Benutzung dieser Schnittstelle wird ausführlich im Administratorhandbuch beschrieben [AGD_ADM, Abschnitte 7.3 bis 7.6].

Abgrenzung Anwendungskonnektor und Fachmodule

Die Sicherheitsfunktionalität SF.Administration/AK ist ebenfalls dafür verantwortlich, die Konfigurationsparameter der Fachmodule des Konnektors zu managen. Auch für die Konfigurationsparameter der Fachmodule wird die Managementschnittstelle des Konnektors verwendet. Die Web Application zur Administration unterstützt dies ebenfalls. Die Validierung und Prüfung der Konfigurationsparameter für ein Fachmodul erledigt allerdings nicht der Anwendungskonnektor, sondern das Fachmodul selbst. Der Anwendungskonnektor reicht die Konfigurationsparameter an das Fachmodul weiter. Das Fachmodul prüft die Parameter und ruft die TUCs an LS.FM.RMI auf, um sie dem Anwendungskonnektor zum Persistieren zurückzugeben. Die Konnektor Security Guidance erklärt den Vorgang genauer [AGD_Kon-Sec, Abschnitt 3.4.].

Über die Managementanwendung kann auch die Konfiguration des TOE sicher exportiert werden. Die Konfigurationsdaten werden dabei symmetrisch verschlüsselt.

Umgesetzte SFR		
FMT_SMR.1/AK	FMT_SMF.1/AK	FMT_MOF.1/AK
FMT_MTD.1/AK.Admin	FMT_MSA.1/AK.TLS	FMT_MSA.3/AK.TLS

Update der Firmware

Die Managementanwendung stellt Funktionen zur Administration des Gesamtkonnektors, z. B. die Downloads der Updates vom KSR-Server oder die Anpassung des Funktionsumfangs des Konnektors zur Verfügung.

Das Schutzprofil räumt die Möglichkeit ein, dass der TOE automatische Updates seiner Firmware durchführt, wenn ein Administrator diese Funktion an der Management-Schnittstelle nicht deaktiviert hat. Die KoCoBox MED+ setzt die automatische Anwendung von Update-Paketen gemäß A_18390 und

A_18391 um. Der Administrator kann die automatische Aktualisierung für den Konnektor und jedes angeschlossene Kartenterminal gemäß TIP1-A_4835-02 einzeln aktivieren oder deaktivieren.

Der Update-Prozess der Firmware des Konnektors besteht aus zwei Teilen: Dem Einbringen der Update-Dateien in den Konnektor und dem Verarbeiten des Updates. Letzteres ist Aufgabe des Netzkonnektors und wird von der Sicherheitsfunktion SF.Administration/NK erbracht (vgl. Abschnitt 7.1.6).

Die Verbindung des Konnektors zum KSR-Server, der die Updatepakete bereitstellt, erfolgt TLS-gesichert über LS.VPN_TI. TLS wird in der KoCoBox MED+ von der Sicherheitsfunktion SF.CryptographicServices/NK umgesetzt. Für den Download der Update-Files wird eine einseitig authentisierte TLS-Verbindung zum KSR Server aufgebaut. Die Konfigurationsparameter für die Verbindung zum KSR-Server sind in Tabelle 7.5 aufgelistet.

Ein Updatepaket für den Konnektor enthält die Firmware für den Basiskonnektor und die Fachmodule. Eine Aktualisierung des Basiskonnektors enthält immer auch eine Aktualisierung der Fachmodule, diese Updates sind nicht separat voneinander einspielbar. Umgekehrt gilt, dass Fachmodule immer nur im Kontext der Updates des Basiskonnektors aktualisiert werden können. Tabelle 1.7 zeigt die Versionsnummern des TOE und der Fachmodule.

Laufzeitverlängerung für Zertifikate der gSMC-K

Die Sicherheitsfunktion sorgt dafür, dass die Zertifikate der drei gSMC-K des TOE erneuert werden können. Der TSP stellt über die Komponenten-PKI der gematik Zertifikate bereit, deren Laufzeit bis Ende 2025 geht. So kann der Austausch der Konnektoren aufgrund abgelaufener Zertifikate verhindert werden. Das Verfahren ist von der gematik spezifiziert [gemF_LZV_gSMC-K]. Im TOE sorgt die Funktion SF.Administration/AK für das Einbringen der Zertifikate O_Zertifikat_gSMC-K in den Konnektor. Die Zertifikate werden entweder automatisch vom Downloadpunkt in der TI heruntergeladen oder über die Managementschnittstelle in den TOE hochgeladen. SF.Administration/AK überprüft die Daten gemäß TUC_KON_410, wobei auch der Zertifikatsdienst aus SF.CryptographicServices/NK herangezogen wird, um die Zertifikate nach TUC_KON_037 zu prüfen. Im Erfolgsfall speichert der AK die Zertifikate der beiden ihm zugeordneten gSMC-K#2 und gSMC-K#3. in seinem Bereich des sicheren Speichers. Das Zertifikat C.NK.VPN hingegen übergibt der AK an den Netzkonnektor, der es wiederum in seinem eigenen sicheren Speicher ablegt. Dadurch, dass der AK die Gültigkeitsprüfung unternommen hat, muss der NK dies nicht erneut erledigen.

Umgesetzte SFR		
FDP_ACC.1/AK.Update	FDP_ACF.1/AK.Update	FDP_UIT.1/AK.Update

7.2.12. Selbstschutz (SF.SelfProtection/AK)

Der Konnektor verfügt über Schutzmechanismen, um sich selbst und die verarbeiteten Daten zu schützen. Die verschiedenen Mechanismen werden in diesem Abschnitt beschrieben.

Überwachung des Betriebszustands

Der Betriebszustand des TOE wird während des gesamten Betriebsablaufs überwacht. Wenn ein Modul oder ein Dienst einen relevanten[5] Fehler feststellt, wird ein interner Ereignisdienst aufgerufen, um alle anderen Dienste und registrierte Nachrichtenempfänger darüber zu informieren. Die Module entscheiden nach dem Empfang einer Nachricht, ob sie ihre Ausführung unterbrechen, solange der Feh-

[5] Die gematik Spezifikation definiert die kritischen Fehlerzustände, vgl. [gemSpec_Kon, Abschnitt 3.3, TAB_KON_503]

TLS Parameter	Belegung
TLS ID	TLS.1
Schnittstelle	LS.LAN.HTTP_MGMT
Rolle des TOE	Server
Peer	Browser
Protokoll	HTTP
Port	9443
TOE authentisiert	✓
Identität des Peer	Benutzername/Passwort
Authentifizierung des Peer durch	AdminService::Core

Tabelle 7.4.: TLS Parameter für die Verbindung zur Management-Webanwendung

TLS Parameter	Belegung
TLS ID	TLS.11
Schnittstelle	LS.VPN_TI.HTTP
Rolle des TOE	Client
Peer	KSR Update Server
Protokoll	HTTP
Port	dyn.
TOE authentisiert	.
Identität des Peer	C.ZD.TLS-S, 1.2.276.0.76.4.160
Authentifizierung des Peer durch	CertificateService::Core

Tabelle 7.5.: TLS Parameter für die Verbindung zum KSR-Service

lerzustand besteht. Diese Entscheidung wird anhand der Regeln aus der Spezifikation [gemSpec_Kon, TAB_KON_504] getroffen.

Umgesetzte SFR
FPT_FLS.1/AK

Selbsttests

Der Konnektor führt beim Systemstart einen Selbsttest durch. Der Administrator kann den Selbsttest während der Laufzeit erneut starten. Der Selbsttest findet auch alle 24 Stunden statt (vgl. das entsprechende SFR des Netzkonnektors FPT_TST.1/NK). Der ST-Anwendungshinweis dort gilt entsprechend auch für den AK. Die Prüfung bezieht sich nicht streng auf ausführbare Dateien, sondern auch alle anderen Teil der Firmware. Damit gilt der Integritätsschutz auch für die XML-Schemadateien, aus denen sich die Signaturrichtlinien zusammensetzen.

Umgesetzte SFR	
FPT_TST.1/AK.Run-time	FPT_TST.1/AK.Out-Of-Band

Löschung sensibler Daten aus dem Arbeitsspeicher

Das im TOE verwendete Java Runtime Environment ist speziell für die Belange des Konnektors gehärtet worden. Es wird dafür gesorgt, dass nicht mehr benötigte kryptographische Schlüssel unmittelbar nach der Verwendung sicher gelöscht werden. Dabei werden die Speicherbereiche, in den die Schlüssel lagen, mit konstanten Werten überschrieben. Der Garbage Collector der JRE wurde so angepasst, dass keine Schattenkopien mehr im Speicher verbleiben.

Umgesetzte SFR
FDP_RIP.1/AK

Die kryptographische Identität des Konnektors ist auf einer gSMC-K gespeichert. Diese Smart Card erfüllt die Anforderungen des Schutzprofils [BSI-CC-PP-0082-2] und gehört zur Einsatzumgebung. Die Schutzmechanismen werden hier nicht weiter betrachtet.

7.2.13. Protokollierungsdienst/AK (SF.Audit/AK)

Sicherheitsrelevante Ereignisse des Konnektors und der Fachmodule werden in einem Protokoll permanent gespeichert. Der Speicherplatz für dieses Protokoll ist mit 900 MB angemessen groß. Beim Überlauf des Protokollspeichers werden alte Protokolleinträge zyklisch überschrieben, also die ältesten Einträge zuerst. Es gibt keinen anderen Mechanismus zum Löschen oder Ändern von Protokolleinträgen. Zum Schutz der Log-Einträge geben die Konfigurationsparameter *LOG_DAYS* (für den Basiskonnektor) und *FM_<fmName>_LOG_DAYS* (für Fachmodule) an, nach wievielen Tagen Logeinträge frühestens überschrieben werden können [gemSpec_Kon, TAB_KON_609]. Die Konfigurationsparameter *LOG_LEVEL FM_<fmName>_LOG_LEVEL* legt die Mindest-Schwere zu protokollierender Einträge fest.

Umgesetzte SFR	
FAU_STG.4/AK	FAU_STG.1/AK

Der TOE ist gegen Überlauf seines Protokollspeichers geschützt. Extern ausgelöste Audit-Ereignisse werden direkt abgespeichert, falls dasselbe Ereignis nicht bereits innerhalb der letzten zwei Sekunden aufgetreten ist. Trat das Ereignis bereits in den letzten zwei Sekunden auf, wird nur der Zähler erhöht. Wenn das Ereignis danach innerhalb von zwei Sekunden nicht erneut auftritt, wird es aus der Liste entfernt und beim nächsten Auftreten als ein neues Ereignis behandelt. Wenn ein Ereignis mehrfach auftritt und der Zähler mehrfach inkrementiert wird, wird das Ereignis nach 20 Sekunden (maximale Höhe des Zählers) erneut protokolliert. Die Logs werden in einer Datenbank gespeichert und automatisch verschlüsselt (vgl. SF.CryptographicServices/NK).

Wenn der Protokollspeicher des TOE zu mehr als 80% gefüllt ist, informiert der TOE den Administrator über das Display am Gehäuse des Konnektors.

Der Protokollspeicher kann nur vom zentralen Protokollierungsdienst, nicht aber von externen Entitäten, ausgelesen werden. Zum Betrachten der Protokolleinträge greift der Administrator auf Funktionen der Managementschnittstelle zurück, die die zu präsentierenden Einträge beim Protokollierungsdienst anfordert.

Die Managementoberfläche des Konnektors bietet dem Administrator die Möglichkeit, das Sicherheitsprotokoll zu betrachten (vgl. [AGD_ADM, Abschnitt 7.5.6]).

Umgesetzte SFR		
FAU_GEN.1/AK	FAU_SAR.1/AK	FPT_STM.1/AK

7.3. TOE Sicherheitsfunktionen für Fachmodule

Für die Fachmodule implementiert der TOE Sicherheitsfunktionalitäten, die gemäß Spezifikation vom Basiskonnektor umgesetzt werden müssen.

7.3.1. VAU-Protokoll (SF.VAU)

Das von der gematik entwickelte VAU-Protokoll dient zur Ende-zu-Ende-Verschlüsselung der Kommunikation zwischen dem TOE und der vertrauenswürdigen Ausführungsumgebung [gemSpec_Krypt, Kapitel 6]. Dieser Endpunkt wird in diesem Security Target „VAU-Server-Endpunkt“ benannt. Der Konnektor ist immer Client einer VAU-Verbindung.

Diese Zusammenfassung zeigt, welche SFR die Anforderungen aus den einzelnen Protokollschritten abdecken. Dabei liegt der Fokus der Beschreibung auf den sicherheitsrelevanten Eigenschaften des Protokolls. Grundsätzlich folgt das VAU-Protokoll dem *fail fast*-Ansatz. Sobald einer der Kommunikationspartner eine Unregelmäßigkeit bemerkt, muss dieser die entsprechenden Fehlermeldungen senden und die Kommunikation beenden. Es ist nicht erlaubt, die Kommunikation durch Fall-Backs wie erneute Versuche oder reduzierte kryptographische Stärke aufrecht zu erhalten.

7.3.1.1. Allgemeiner Protokollablauf

Der TOE setzt die Clientseite des VAU-Protokolls um. Der gesamte allgemeine Protokollablauf wird durch die Umsetzung der Sicherheitsanforderung FTP_ITC.1/VAU erfüllt. Die allgemeinen Parameter für den Ablauf und die Verwendung des HTTP-Protokolls beim Transport der VAU-Protokoll-Nachrichten definieren A_15549, A_16884 und A_17074, sowie A_20549 und A_18466-01. Im Fehlerfall muss der TOE anforderungskonform mit einem Abbruch reagieren. Die Anforderungen A_16900 und A_16849 beschreiben das Verfahren.

Im Rahmen des *Handshakes* muss der TOE zwei Nachrichtentypen generieren und versenden: *VAUClientHello* (A_16883-01, A_16897) und *VAUClientSigFin* (A_17070-02, A_17071). Weiterhin muss der TOE die Handshake-Nachrichten *VAUServerHello* (A_16903, A_16941-01) und *VAUServerSigFin* (A_17084) des Servers interpretieren.

Beim *Nutzdatentransport* muss der TOE die Anforderungen A_16945-02, A_16957-01, A_16958 und A_17069 umsetzen. Für die Datenübertragung mit MTOM muss der TOE A_18465-01 implementieren.

Umgesetzte SFR
für alle genannten Afos: FTP_ITC.1/VAU

7.3.1.2. VAUClientHello

In Anforderung A_16883-01 wird der Aufbau der vom TOE zu sendenden *VAUClientHello*-Nachricht zur Initiierung einer VAU-Verbindung beschrieben.

Dabei muss der TOE ein Schlüsselpaar basierend auf brainpoolP256r1 generieren. Dieses Schlüsselpaar wird für jede Verbindung neu generiert, unabhängig davon, ob der TOE in der Test- oder in der Produktivumgebung eingesetzt wird (vgl. A_21888). Der öffentliche Punkt des ephemeren ECDH-Schlüsselpaares wird im Feld *PublicKey* der Antwortnachricht Base64-kodiert eintragen. Das DER-kodierte X.509-Client-Zertifikat inkl. der äußeren Zertifikatssignatur wird anschließend gehashed. Der SHA-256 Hashwert wird Base64-kodiert. Diese Kodierung wird als Wert im Feld *CertificateHash* der Antwortnachricht eingetragen. Die gesamte Datenstruktur wird zur späteren Verwendung erneut gehasht (*VAUClientHelloDataHash*). Den Versand der *VAUClientHello*-Nachricht an den VAU-Server beschreibt A_16897.

Umgesetzte SFR	
für A_16883-01:	FCS_CKM.1/VAU
	FCS_COP.1/VAU.Hash
	FTP_ITC.1/VAU
für A_16897	FTP_ITC.1/VAU

7.3.1.3. VAUServerHello

Beim Empfang der *VAUServerHello*-Nachricht fordert Anforderung A_16903, dass der TOE den Hashwert über *VAUClientHelloDataHash* aus der Server-Nachricht mit dem selbst berechneten Hashwert vergleicht. Stimmen die Werte nicht überein, wird das Protokoll abgebrochen.

In Anforderung A_16941-01 wird gefordert, dass der Client die Signatur über dem Feld *Data* prüft. In diesem Zuge muss das Zertifikat des Servers ebenfalls geprüft werden. Dabei muss auch die Signatur des Zertifikats verifiziert werden. A_17081 schreibt vor, dass der Server die VAU-Server-Identität oid_epa_vau verwenden muss. Die Konnektor-Spezifikation definiert in A_17225-01 die Prüfregeln für das Zertifikat des Servers. Zusätzlich nennt A_15210 [gemSpec_FM_ePA] spezielle Prüfregeln für das Zertifikat, die der Konnektor gemäß Technischer Richtlinie für das Fachmodul ePA [TR-03157] ausführen muss. Auch hier wird der Hashwert des übergebenen Zertifikats berechnet.

Umgesetzte SFR	
für A_16903:	FCS_COP.1/VAU.Hash
für A_16941-01:	FCS_COP.1/VAU.ECDSA
	FPT_TDC.1/VAU.Zert
	FCS_COP.1/VAU.Hash
für A_17081:	FPT_TDC.1/VAU.Zert
für A_15210:	FPT_TDC.1/VAU.Zert
für A_17225-01:	FPT_TDC.1/VAU.Zert

7.3.1.4. Schlüsselableitung mit ECDH und HKDF

In den Anforderungen A_16852-01 und A_16943-01 wird gefordert, dass der TOE mittels ECDH und der HKDF drei AES-Schlüssel ableitet, mit denen in der Folge die zu übermittelnden Daten ver- und die empfangenen Daten entschlüsselt werden. Dabei ist vom TOE zu prüfen, ob der vom VAU-Server-Endpunkt übermittelte Kurvenpunkt tatsächlich auf der Kurve brainpoolP256r1 liegt. Der so abgeleitete Schlüssel darf maximal 24 Stunden verwendet werden, danach bricht der TOE die Verbindung ab (A_15549). Durch einen erneuten Verbindungsaufbau muss ein neuer AES-Schlüssel ausgehandelt werden. Das passiert nicht automatisch. Der TOE weicht in dieser Hinsicht von der Spezifikation ab. Das aufrufende Fachmodul erhält eine passende Fehlermeldung, wenn es einen nach dem Timeout abgebauten VAU-Kanal erneut verwenden möchte.

Umgesetzte SFR	
für A_16852-01:	FCS_CKM.1/VAU
für A_16943-01:	FCS_CKM.1/VAU
für A_15549:	FTP_ITC.1/VAU

7.3.1.5. VAUClientSigFin

Anforderung A_17070-02 definiert den Aufbau der *VAUClientSigFin*-Nachricht. Im Speziellen wird gefordert, dass der TOE wiederum Hashwerte berechnen und Teile der Nachricht AES-GCM-256 verschlüsseln muss. Das zufällige Element des Initialisierungsvektors wird vom sicheren Zufallsgenerator erzeugt.

Die beiden konkatenierten Base64-kodierten Hashwerte werden mit dem AUT-Zertifikat der SMC-B gemäß A_17081 signiert.

A_17081 fordert, dass das AUT-Schlüsselmaterial einer eGK oder einer SMC-B verwendet werden muss. Den Versand der Nachricht beschreibt A_17071.

Umgesetzte SFR	
für A_17070-02:	FCS_COP.1/VAU.AES
	FCS_RNG.1/Hash_DRBG
	FCS_COP.1/VAU.Hash
	FTP_ITC.1/VAU
für A_17081:	FCS_COP.1/VAU.ECDSA
für A_17071	FTP_ITC.1/VAU

7.3.1.6. VAUServerFin

Anforderung A_17084 definiert, dass der Client prüfen muss, ob die *VAUServerFin*-Nachricht protokollkonform ist.

Umgesetzte SFR	
für A_17084	FTP_ITC.1/VAU

7.3.1.7. Nutzerdatentransport

In Anforderung A_16945-02 wird gefordert, dass der TOE die Nutzerdaten ver- und entschlüsselt. Dies geschieht mit AES-GCM-256.

Aus Gründen der Performanz können größere Daten mittels MTOM/XOP-Kodierung transportiert werden. Dabei werden die Binärdaten nicht Base64 innerhalb einer XML-Datenstruktur kodiert, sondern beim HTTP/SOAP-Request (bzw. bei der -Response) über eine MIME-Multipart-Kodierung innerhalb von HTTP.

Der VAU-Client führt einen unsigned 64-Bit-Nachrichtenzähler, der vor Replay-Attacken schützen soll. Dieser startet mit dem Wert 1 und wird bei jeder abgeschickten Nachricht um 2 erhöht wird.

Der VAU-Client erzeugt zunächst einen Initialisierungsvektor (IV). Das 32-Bit lange zufällige Element des IV wird vom sicheren Zufallsgenerator des Basiskonnektors erzeugt. Der komplette 96-Bit Initialisierungsvektor setzt sich aus dem 32-Bit zufälligem Element und dem 64-Bit Nachrichtenzähler zusammen.

Unter Verwendung dieses IV und des zweiten aus A_16943-01 abgeleiteten Schlüssel (Client-to-Server-Schlüssel) wird die Nachricht verschlüsselt. Der Client berechnet so den *Ciphertext*.

Die Ausgangsnachricht, bestehend aus einer 256-Bit KeyID dem 96-Bit Initialisierungsvektor mit *Ciphertext* und einem 128-Bit Authentication-Tag, wird per HTTP-POST-Request mit Content-Type *application/octet-stream* ohne weitere Kodierungen versendet.

VAUResponses werden hinsichtlich Einhaltung der maximalen Größe eines Dokuments, der maximalen Gesamtgröße aller Dokumente und des erlaubten Encodings validiert. Im Fehlerfall wird die Verarbeitung abgebrochen.

Umgesetzte SFR	
für A_16945-02:	FCS_COP.1/VAU.AES
	Benutzt FCS_RNG.1/Hash_DRBG

7.3.2. SGD-Protokoll / ECIES-Verfahren (SF.SGD)

Die Autorisierung zum Zugriff auf Daten der Dokumentenverwaltung erfolgt über kryptographische Berechtigungen, die in der Autorisierungskomponente des ePA-Aktensystems doppelt verschlüsselt hinterlegt werden. Zum Ver- und Entschlüsseln des Schlüsselmaterials muss der TOE – im Auftrag des Fachmoduls ePA – mit den Schlüsselgenerierungsdiensten (SGD) der TI kommunizieren. Die Schlüsselgenerierungsdienste 1 und 2 (im folgenden: SGD 1 und SGD 2) halten jeweils einen der Schlüssel vor, mit denen das Schlüsselmaterial des Aktensystems dechiffriert werden kann. Der TOE kommuniziert mit den SGD, um die Schlüssel von dort zu erhalten. Die Kommunikation zwischen TOE und den SGD muss Ende-zu-Ende verschlüsselt sein, um Integrität, Vertraulichkeit und Authentizität zu wahren.

Das Protokoll für diese Kommunikation ist das SGD-Protokoll. Es wurde von der gematik entwickelt und basiert auf dem „Elliptic Curve Integrated Encryption Scheme (ECIES)“ [TR-02102-1]. Das Verfahren wird in der Spezifikation des Schlüsselgenerierungsdiensts [gemSpec_SGD_ePA, Abschnitt 2.3 und Kapitel 9] beschrieben, die kryptographischen Eigenschaften in [gemSpec_Krypt, Abschnitt 3.15.5].

7.3.2.1. Allgemeiner Protokollablauf

In diesem Abschnitt werden der allgemeine Protokollablauf und die dazu gehörenden Anforderungen auf SFR abgebildet. Der TOE ist immer Client in diesem Protokoll, Server ist immer der Schlüsselgenerierungsdienst. Der TOE bedient die HTTPS-Schnittstellen des SGD, die in A_17889 definiert werden. Diese Anforderung ist nicht normativ für den Client, spezifiziert aber die Parameter der Schnittstelle, die der Client bedienen muss. Die grundlegenden Parameter der JSON-Strukturen werden in A_17892 und A_17893 definiert.

Der Zugriff auf die Schlüssel erfolgt in drei Aufrufen. Die im folgenden verwendete Nummerierung der Schritte entspricht derjenigen in Abschnitt 2.3 der Spezifikation des Schlüsselgenerierungsdienstes.

Wie beim VAU-Protokoll subsumiert ein einziger SFR die Forderung nach einer korrekten Implementierung des Protokolls in allen Schritten. Auch hier gilt, dass ein Fehler in der Verarbeitung oder eine fehlgeschlagene Validierung eines Datums zum sofortigen Abbruch des Protokolls führt. Die Anforderungen A_18987, A_18988 und A_19000 spezifizieren die Reaktion der Kommunikationspartner auf Fehler in der Protokollausführung.

Umgesetzte SFR
FTP_ITC.1/SGD

7.3.2.2. Holen des öffentlichen Schlüssels des SGD

In den Schritten 1 (für SGD 1) und 4 (für SGD 2) holt der TOE mit der Operation *GetPublicKey* den öffentlichen Schlüssel des SGD-HSM und erfüllt damit A_17897. Das Nachrichtenformat wird in A_17895-01 definiert. Der TOE erhält das signierte Zertifikat und den ECIES-Schlüssel. Der TOE prüft diese gemäß A_18024. Im Rahmen dieser Prüfung muss der TOE die ordnungsgemäße Kodierung des ECIES-Schlüssels feststellen, die A_17899 und A_17894-01 fordern.

Umgesetzte SFR	
für A_17895-01:	FTP_ITC.1/SGD
für A_17897:	FTP_ITC.1/SGD
für A_17894-01:	FDP_ITC.2/SGD
für A_17899:	FDP_ITC.2/SGD
	FDP_ACC.1/SGD
	FDP_ACF.1/SGD
für A_18024:	FDP_ITC.2/SGD
	FPT_TDC.1/SGD.Zert
	FCS_COP.1/SGD.ECDSA
	FDP_ACC.1/SGD
	FDP_ACF.1/SGD
für A_19971:	FCS_COP.1/SGD.Hash

7.3.2.3. Anfordern des Authentisierungstokens

Vor dem Aufruf der Funktion *getAuthenticationToken* muss der TOE als Client einige Vorbereitungen erfüllen. In Schritt 7 werden die Hashwerte über die ECIES-Schlüsselwerte der beiden SGD-HSM berechnet. Dies ist eine Vorbereitung für die Erfüllung der Anforderung A_17900. In Schritt 8 erzeugt der TOE ein ephemeres ECIES-Schlüsselpaar mit den Kurven-Parametern der brainpoolP256r1 gemäß A_17874. Dabei stellt der TOE sicher, dass der Punkt des öffentlichen Schlüssels auf derselben elliptischen Kurve liegt wie der Punkt des Empfängers (A_17903). Die Signatur des Schlüssels und der Hashwerte erfolgt gemäß A_17901 durch eine Karte in der Umgebung des TOE und wird hier nicht durch einen SFR abgebildet (vgl. ST-Anwendungshinweis zu FCS_COP.1/SGD.ECDSA). Das ephemere Schlüsselpaar wird nur für eine Schlüsselableitung verwendet, der TOE bewahrt es nicht auf. Nach Ablauf der Operation wird der Schlüssel durch den Garbage Collector vernichtet.

Umgesetzte SFR	
für A_17900:	FCS_COP.1/SGD.Hash
für A_17874:	FCS_COP.1/SGD.ECIES
für A_17874:	Umgebung, ST-Anwendungshinweis zu FCS_COP.1/SGD.ECDSA
für A_17901:	Umgebung, ST-Anwendungshinweis zu FCS_COP.1/SGD.ECDSA
für A_18005:	Benutzt FCS_CKM.4/AK
für A_19971:	FCS_COP.1/SGD.Hash

In den Schritten 9 (für SGD 1) und 14 (für SGD 2) fordert der TOE das Token über die Operation *GetAuthenticationToken* an. A_18021 beschreibt das Format der Nachricht. Die an den SGD-HSM zu übergebende Challenge enthält gemäß A_18025-01 neben dem Wort *Challenge* und genau zwei Leerzeichen zwei Elemente: Zuerst eine hexadezimal kodierte 256 Bit lange Zufallszahl, die der TOE über den sicheren Zufallsgenerator gemäß FCS_RNG.1/Hash_DRBG erzeugt; als zweites Element folgt der ebenfalls hexadezimal kodierte SHA-256 Hashwert aus der Aneinanderreihung des eigenen ECIES-Schlüssels und dem DER-kodierten AUT-Zertifikat, mit dem der ECIES-Schlüssel signiert wurde.

In den Nutzdaten des Requests wird der öffentliche ECIES-Schlüssel des TOEs übertragen, wie von A_17902 spezifiziert. Die Nachricht wird nach dem ECIES-Verfahren verschlüsselt. Die Spezifikation definiert das Verfahren in A_17875, in der die Schlüsselableitung mit ECDH und HKDF und die Verschlüsselung mit AES-GCM gefordert wird. Die Antwort des SGD-HSM wird gemäß A_18028 entschlüsselt und geprüft (Schritte 11 für SGD 1 und 17 für SGD 2).

Umgesetzte SFR	
für A_18021:	FTP_ITC.1/SGD
für A_18025-01:	Benutzt FCS_RNG.1/Hash_DRBG
für A_17875:	FCS_COP.1/SGD.ECIES, FCS_COP.1/SGD.ECDSA
für A_17902:	FCS_COP.1/SGD.ECIES
für A_17903:	FCS_COP.1/SGD.ECIES
für A_18028:	FTP_ITC.1/SGD FCS_COP.1/SGD.Hash

7.3.2.4. Ableitung des Schlüsselmaterials

Im letzten Aufruf des Ablaufs fordert der TOE bei SGD 1 und SGD 2 jeweils einen der beiden Schlüssel an, die benötigt werden, um den Akten- und Kontextschlüssel der Dokumentenverwaltung zu entschlüsseln[6]. Dazu verwendet der TOE gemäß A_17888 und A_17898 die Operation *KeyDerivation* des Schlüsselgenerierungsdienst (Schritt 12 für SGD 1 und 17 für SGD 2). A_18029 beschreibt den Aufbau der Nachricht. Für diesen Schritt übermittelt der TOE drei Elemente an den SGD: Eine vom sicheren Zufallsgenerator erzeugte Request ID, das Authentisierungstoken aus dem vergangenen Schritt und eine Ableitungsregel, die gemäß A_17924-01 erzeugt wird. Wenn in der Ableitungsregel die Telematik ID einer LEI enthalten ist, wird diese gemäß A_18003 transformiert. Eine KVNR wird gemäß A_18006 eingebracht. Die Nachricht wird mit ECIES verschlüsselt und an den Schlüsselgenerierungsdienst gesendet (Kodierung nach A_17902, ECIES wieder gemäß A_17875, Konkordanz der Kurven gemäß A_17903).

Der TOE erhält die Antwort ebenfalls verschlüsselt, er wendet das ECIES-Verfahren an, um die Nachricht des Servers zu entschlüsseln. Das Format der Nachricht und die Prüfregeln sind in A_18031-01 definiert. Der TOE muss prüfen, ob die Nachricht dem spezifizierten Format entspricht. Zusätzlich fordert A_17924-01, dass der TOE diese Nachrichten korrekt interpretiert. Die drei im Request übermittelten Elemente Request ID, Authentisierungstoken und Ableitungsregel müssen identisch in der Antwortnachricht des Schlüsselgenerierungsdienst enthalten sein. Ist dies nicht der Fall verwirft der TOE die Antwort und bricht die Protokollaushandlung ab. Zusätzlich präzisiert A_20977 die Prüfung der Ableitungsregeln. Die gesendete und die erhaltene Ableitungsregel müssen bitgenau identisch sein.

Schließlich enthalten die entschlüsselten Nutzdaten den Berechtigungsschlüssel für den Zugriff auf das Aktensystem.

Umgesetzte SFR	
für A_17888:	FTP_ITC.1/SGD
für A_17898:	FTP_ITC.1/SGD
für A_17924-01:	FTP_ITC.1/SGD
für A_18003:	FTP_ITC.1/SGD
für A_18006:	FTP_ITC.1/SGD
für A_18029:	FTP_ITC.1/SGD
	Benutzt FCS_RNG.1/Hash_DRBG
für A_17875:	FCS_COP.1/SGD.ECIES,
	FCS_COP.1/SGD.ECDSA
für A_17902:	FCS_COP.1/SGD.ECIES
für A_17903:	FCS_COP.1/SGD.ECIES
für A_18031-01:	FTP_ITC.1/SGD
für A_20977:	FTP_ITC.1/SGD

[6] Begriffsklärung: Die Ableitung des Schlüssels erfolgt im Schlüsselgenerierungsdienst. Die Ableitung der ECIES-Schlüssel mittels ECDH, die in FCS_COP.1/SGD.ECIES modelliert sind, wird dabei nicht angewendet.

7.4. Verhältnis von SFR zu SF des Netzkonnektors

Tabelle 7.6 zeigt, in welchem Verhältnis die im Abschnitt 6.2 definierten Sicherheitsanforderungen an den Netzkonnektors zu den in Abschnitt 7.1 beschriebenen Sicherheitsfunktionen des NK stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	SF.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	.	.	✓	.	.	.	.

Abbildung der SFR des NK auf Sicherheitsfunktionalitäten (Forts.)

	SF.DynamicPacketFilter	SF.NetworkServices	SF.Administration/NK	SF.Audit/NK	SF.CryptographicServices/NK	SF.SelfProtection/NK	SF.VPN
FMT_SMR.1/NK	.	.	✓	.	.	.	.
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 7.6.: Abbildung der SFR des NK auf Sicherheitsfunktionalitäten

7.5. Verhältnis von SFR zu SF des Konnektors

Tabelle 7.7 zeigt, in welchem Verhältnis die im Abschnitt 6.3 definierten Sicherheitsanforderungen an den Anwendungskonnektors zu den in Abschnitt 7.2 beschriebenen Sicherheitsfunktionen des AK stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	SF.AccessControl	SF.Administration/AK	SF.Audit/AK	SF.CryptographicServices/AK	SF.SelfProtection/AK	SF.Authentication	SF.CardTerminalMgmt	SF.EncryptionService	SF.SecureStorage	SF.SGD	SF.SignatureService	SF.SmartCardMgmt	SF.TLS	SF.VAU	SF.VSDM
FAU_GEN.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FAU_SAR.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FAU_STG.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FAU_STG.4/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FCS_CKM.1/AK.AES	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.
FCS_CKM.1/VAU	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
FCS_CKM.4/AK	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/AK.AES	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/AK.CMS.Ent	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/AK.CMS.Sign	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.CMS.SigPr	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.CMS.Ver	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/AK.ECIES	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/AK.PDF.Sign	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.PDF.SigPr	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.SHA	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.BNetzA-VL	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.
FCS_COP.1/AK.SigVer.ECDSA	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.SigVer.PSS	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.SigVer.SSA	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.XML.Ent	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/AK.XML.Sign	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.XML.SigPr	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/AK.XML.Ver	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/SGD.ECDSA	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/SGD.ECIES	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/SGD.Hash	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/VAU.AES	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
FCS_COP.1/VAU.ECDSA	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
FCS_COP.1/VAU.Hash	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
FDP_ACC.1/AK.eHKT	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.

Abbildung der SFR des AK auf Sicherheitsfunktionalitäten (Forts.)

	SF.AccessControl	SF.Administration/AK	SF.Audit/AK	SF.CryptographicServices/AK	SF.SelfProtection/AK	SF.Authentication	SF.CardTerminalMgmt	SF.EncryptionService	SF.SecureStorage	SF.SGD	SF.SignatureService	SF.SmartCardMgmt	SF.TLS	SF.VAU	SF.VSDM
FDP_ACC.1/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACC.1/AK.Infomod	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ACC.1/AK.KD	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_ACC.1/AK.PIN	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_ACC.1/AK.SDS	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACC.1/AK.Sgen	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACC.1/AK.SigPr	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACC.1/AK.TLS	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_ACC.1/AK.Update	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ACC.1/AK.VSDM	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
FDP_ACC.1/SGD	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_ACF.1/AK.eHKT	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ACF.1/AK.Infomod	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.KD	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_ACF.1/AK.PIN	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
FDP_ACF.1/AK.SDS	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.
FDP_ACF.1/AK.Sgen	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACF.1/AK.SigPr	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ACF.1/AK.TLS	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_ACF.1/AK.Update	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FDP_ACF.1/AK.VSDM	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
FDP_ACF.1/SGD	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_DAU.2/AK.Cert	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_DAU.2/AK.QES	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_DAU.2/AK.Sig	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ETC.2/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ITC.2/AK.BNetzA-VL	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FDP_ITC.2/AK.Enc	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
FDP_ITC.2/AK.Sig	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_ITC.2/SGD	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FDP_RIP.1/AK	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
FDP_SDI.2/AK	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FDP_UCT.1/AK.TLS	.	.	.	.	.	.	✓	.	.	.	.	.	✓	.	.
FDP_UIT.1/AK.TLS	.	.	.	.	.	.	✓	.	.	.	.	.	✓	.	.
FDP_UIT.1/AK.Update	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FIA_API.1/AK.TLS	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.

Abbildung der SFR des AK auf Sicherheitsfunktionalitäten (Forts.)

	SF.AccessControl	SF.Administration/AK	SF.Audit/AK	SF.CryptographicServices/AK	SF.SelfProtection/AK	SF.Authentication	SF.CardTerminalMgmt	SF.EncryptionService	SF.SecureStorage	SF.SGD	SF.SignatureService	SF.SmartCardMgmt	SF.TLS	SF.VAU	SF.VSDM
FIA_API.1/AK	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_SOS.1/AK.CS.Passwörter	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_SOS.1/AK.Passwörter	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_SOS.2/AK.Jobnummer	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FIA_SOS.2/AK.PairG	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_UAU.1/AK	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FIA_UAU.5/AK	.	.	.	.	.	✓	.	.	.	.	✓	.	.	.	.
FIA_UID.1/AK	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_MOF.1/AK	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FMT_MSA.1/AK.Infomod	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FMT_MSA.1/AK.TLS	.	✓	.	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_MSA.1/AK.User	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FMT_MSA.1/AK.VSDM	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
FMT_MSA.3/AK.Infomod	✓	.	.	.	.	.	.	.	.	.	.	.	.	.	.
FMT_MSA.3/AK.Sig	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FMT_MSA.3/AK.TLS	.	✓	.	.	.	✓	.	.	.	.	.	.	.	.	.
FMT_MSA.3/AK.VSDM	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓
FMT_MSA.4/AK	.	.	.	.	.	.	.	.	.	.	✓	✓	.	.	.
FMT_MTD.1/AK.Admin	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FMT_MTD.1/AK.eHKT_Abf	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.
FMT_MTD.1/AK.eHKT_Mod	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.
FMT_MTD.1/AK.Zert	.	✓	.	.	.	.	.	.	.	.	.	✓	.	.	.
FMT_SMF.1/AK	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FMT_SMR.1/AK	.	✓	.	.	.	.	.	.	.	.	.	.	.	.	.
FPT_FLS.1/AK	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
FPT_STM.1/AK	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	.
FPT_TDC.1/AK	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
FPT_TDC.1/SGD.Zert	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FPT_TDC.1/VAU.Zert	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
FPT_TEE.1/AK	.	.	.	.	.	.	✓	.	.	.	.	✓	.	.	.
FPT_TST.1/AK.Out-Of-Band	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
FPT_TST.1/AK.Run-time	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.
FTA_TAB.1/AK.Jobnummer	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FTA_TAB.1/AK.SP	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FTP_ITC.1/AK.CS	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FTP_ITC.1/AK.eHKT	.	.	.	.	.	.	✓	.	.	.	.	.	✓	.	.
FTP_ITC.1/AK.FD	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.

Abbildung der SFR des AK auf Sicherheitsfunktionalitäten (Forts.)

	SF.AccessControl	SF.Administration/AK	SF.Audit/AK	SF.CryptographicServices/AK	SF.SelfProtection/AK	SF.Authentication	SF.CardTerminalMgmt	SF.EncryptionService	SF.SecureStorage	SF.SGD	SF.SignatureService	SF.SmartCardMgmt	SF.TLS	SF.VAU	SF.VSDM
FTP_ITC.1/AK.KSR	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FTP_ITC.1/AK.QSEE	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
FTP_ITC.1/AK.TSL	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FTP_ITC.1/AK.VZD	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
FTP_ITC.1/SGD	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
FTP_ITC.1/VAU	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.

Tabelle 7.7.: Abbildung der SFR des AK auf Sicherheitsfunktionalitäten

8. ASE_TSS: Fachmodule

Dieses Kapitel erfüllt die Anforderung des Refinements für ASE_TSS an den *Hersteller*, die in Unterabschnitt 6.4.5 erhoben wird.

Konnektoren dienen als Ablaufplattform für Fachmodule. Die gematik Spezifikation bezeichnet ein Fachmodul als „integrale[n] Bestandteil des Konnektors“. Daraus ergeben sich gegenseitige Anforderungen zwischen Basiskonnektor und den Fachmodulen. Dieses Kapitel geht auf die Anforderungen ein und zeigt, auf welche Weise der Basiskonnektor die Forderungen der Fachmodule umsetzt und welche Funktionen den Fachmodulen zur Verfügung gestellt werden.

Fachmodule unterliegen im Konnektor Restriktionen und Auflagen. Diese werden in der Konnektor Security Guidance beschrieben [AGD_Kon-Sec]. Die dort beschriebenen Composition Requirements müssen vom Entwickler eines Fachmoduls eingehalten werden, um die Funktionsfähigkeit des Gesamtkonnektors nicht zu gefährden. Zur besseren Lesbarkeit werden die Composition Requirements in Anhang C wiederholt.

8.1. Erklärung der Konformität zu Technischen Richtlinien

8.1.1. Fachmodule NFDM und AMTS / PTV 3

Die Technischen Richtlinien der Fachmodule NFDM und AMTS fordern, dass die CC-Zertifizierung des Konnektors bestimmte Eigenschaften des Konnektors umfassen muss [TR-03154; TR-03155, Abschnitt 3.3.2]. Dieses Security Target ist konform zu diesen Anforderungen, vgl. Abschnitt 2.5. Dies sind – neben den TUCs für die Fachmodule (vgl. Abschnitt 8.2) – allgemeiner formulierte Funktionalitäten. Die folgenden Unterabschnitte benennen diese Funktionalitäten und erklären, wie das Security Target die geforderten Eigenschaften sicherstellt.

Konfigurationsparameter

Der Basiskonnektor schützt die Konfigurationsparameter von Fachmodulen vor unbefugter Modifikation. Um dies sicherzustellen, setzt das Security Target folgende Maßnahme um: Die Sicherheitsfunktion SF.Administration/AK managt die Konfigurationsparameter der Fachmodule. Die Benutzung dieser Funktion wird in der Konnektor Security Guidance erklärt und dort durch Composition Requirements formalisiert [AGD_Kon-Sec].

Protokollierungsdienst

Fachmodule können den Basiskonnektor aufrufen, um Log-Nachrichten zu persistieren. Jedes Fachmodul erhält einen eigenen Namensraum, sodass die Nachrichten pro Fachmodul separiert werden. Der Konnektor speichert die Lognachrichten in derselben Datenbank wie sein eigenes Log. Benutzer der Fachmodule können über die Funktionen der Managementschnittstelle das Log auslesen. Maßnahmen des Security Targets stellen sicher, dass die Anforderungen der Fachmodule an den Konnektor umgesetzt werden:

- ST-Anwendungshinweis 63 zu FAU_STG.4/AK präzisiert die Behandlung des Parameters *FM_<fm-Name>_LOG_DAYS*, der vorgibt, wie lange die Mindestdauer für das Vorhalten von Protokolleinträgen ist [gemSpec_Kon, TAB_KON_609]. Die Konnektor Security Guidance definiert das Composition Requirement COMP-REQ-7, das beschreibt, wie der Entwickler der Fachmodule mit Konfigurationsdaten umgehen muss.
- Die Zuweisung an FAU_GEN.1.1/AK sichert zu, dass die Security-relevanten Ereignisse des Fachmoduls vom Protokollierungsdienst des Konnektors erfasst und behandelt werden.

Signaturdienst (nur für NFDM)

Fachmodule können den Signaturdienst des Basiskonnektors nutzen, um QES-Prüfungen von XML-detached Signaturen durchzuführen. Das Security Target stellt dies sicher durch die SFR in Unterunterabschnitt 6.3.3.4, insbesondere FDP_DAU.2.2/AK.QES(1), (2), (4), (5).

Gültigkeitsprüfung der eGK

Der Basiskonnektor prüft die Gültigkeit einer eGK. Dies wird erreicht durch die Erfüllung der Sicherheitsanforderung FPT_TEE.1/AK. Die Erläuterung des Sicherheitsziels O.AK.Chipkartendienst im Schutzprofil präzisiert dieses SFR [BSI-CC-PP-0098, S. 316] und macht deutlich, welche Aspekte des SFR hier einschlägig sind. Die Sicherheitsfunktionalität SF.SmartCardMgmt setzt das SFR um (vgl. Unterabschnitt 7.2.6).

Transportsicherung zwischen Konnektor und Clientsystem

Der Konnektor sichert die Verbindungen zu den Clientsystemen durch TLS ab[1]. Dies wird auf zwei Ebenen erreicht:

- Die Sicherheitsfunktionalität SF.CryptographicServices/NK und die damit assoziierten SFR FTP_ITC.1/NK.TLS, FPT_TDC.1/NK.TLS.Zert, FCS_CKM.1/NK.TLS, FCS_COP.1/NK.TLS.HMAC, FCS_COP.1/NK.TLS.AES, FCS_COP.1/NK.TLS.Auth, FCS_CKM.1/NK.Zert, FDP_ITC.2/NK.TLS und FDP_ETC.2/NK.TLS stellen die kryptographischen Eigenschaften der TLS-Verbindungen bereit.
- Die Sicherheitsfunktionalität SF.TLS managt die Verwendung der TLS-Verbindungen und reagiert auf die entsprechenden Konfigurationsparameter (vgl. Unterabschnitt 7.2.2). Zusätzlich trägt FMT_MOF.1/NK.TLS auch noch Anforderungen an das Management von TLS-Verbindungen bei.

Auslesbarkeit der Version des Konnektors

Die Technischen Richtlinien fordern ein „auslesbare, eindeutige Version des Konnektors sowie des Fachmoduls“. Die Auslesbarkeit ist gegeben über die Managementschnittstelle des TOE. Die Details sind dem Administratorhandbuch zu entnehmen [AGD_ADM, Abschnitte 7.4.1, 7.7.3, 7.7.4].

8.1.2. Fachmodul ePA / PTV 4

Die Technische Richtlinie für das Fachmodul ePA fordert, dass die CC-Zertifizierung des Konnektors bestimmte Eigenschaften des Konnektors umfassen muss [TR-03157, Abschnitt 3.2.2]. Dieses Security Target ist konform zu diesen Anforderungen, vgl. Abschnitt 2.5. Dies sind – neben den TUCs für

[1] Die Verwendung von TLS für die Verbindung zu den Clientsystemen kann abgeschaltet werden. In diesem Fall geht die Verantwortlichkeit für die Sicherstellung der Vertraulichkeit, der Integrität und der Authentizität auf den Leistungserbringer über, vgl. [AGD_ADM, Abschnitt 7.5.1, S. 88ff].

die Fachmodule (vgl. Abschnitt 8.2) – allgemeiner formulierte Funktionalitäten. Die folgenden Unterabschnitte benennen diese Funktionalitäten und erklären, wie das Security Target die geforderten Eigenschaften sicherstellt.

Rollenprüfung im TLS-Dienst

Das Fachmodul ePA definiert beim Verbindungsaufbau für das TLS-Zertifikat der Gegenstelle eine zulässige Rolle. Werden die Anforderungen des Fachmoduls an das Zertifikat der Gegenstelle nicht erfüllt, bricht der Konnektor die Verbindung ab. Die Rollen werden in den Anforderungen

- A_14930 – FM ePA: Authentisierung mit eGK – TLS mit Zertifikats- und Rollenprüfung
- A_14223 – FM ePA: Autorisierung – Verbindung mit Zertifikats- und Rollenprüfung
- A_15532 – FM ePA: Dokumentenverwaltung – TLS mit Zertifikats- und Rollenprüfung

definiert. Der Konnektor setzt diese Anforderung für das Fachmodul durch ein zusätzliches Refinement zu FPT_TDC.1/NK.TLS.Zert um. Das zusätzliche Refinement verweist auf die Anforderung GS-A_4446-05 der Spezifikation [gemSpec_OID].

Rollenprüfung im VAU-Protokoll

Beim Verbindungsaufbau zur VAU führt der Konnektor für das Fachmodul eine Rollenprüfung des Zertifikats der Gegenstelle durch. Weist das Zertifikat der VAU nicht die Rolle oid_epa_vau auf, bricht der Konnektor die Verbindung ab. Dieses Verhalten fordert A_15210 („FM ePA: Dokumentenverwaltung – sichere Verbindung zur VAU mit Zertifikats- und Rollenprüfung“). Der Konnektor setzt diese Anforderung für das Fachmodul durch die Prüung der Rolle in einer Interpretationsregel zu FPT_TDC.1.2/VAU.Zert(2) um.

8.2. Umsetzung der TUCs an LS.FM im Basiskonnektor

Die Technischen Richtlinien fordern die Umsetzung von TUCs aus der Konnektor Spezifikation [gemSpec_Kon]. Tabelle 8.1 zeigt, welche SFR des Konnektors welchen TUC umsetzen. Dies geschieht hier bewusst auf einer abstrakten Ebene. Tabelle 8.2 geht genauer auf die API-Funktionen ein.

Basisdienst	TUC	Beschreibung	SFR
Zugriffsberechtigungsdienst	TUC_KON_000	Prüfe Zugriffsberechtigung	FDP_ACC.1/AK.Infomod, FDP_ACF.1/AK.Infomod
Dienstverzeichnisdienst	TUC_KON_041	Einbringen der Endpunktinformationen während der Bootup-Phase	(keine)
Dokumentenvalidierungsdienst	TUC_KON_080	Dokument validieren (implizit im BK)	FDP_ITC.2/AK.Sig, FMT_MSA.1/AK.User
Kartenterminaldienst	TUC_KON_051	Mit Anwender über Kartenterminal interagieren	FDP_ACC.1/AK.eHKT, FDP_ACF.1/AK.eHKT
	TUC_KON_056	Karte anfordern	(keine)
	TUC_KON_057	Karte auswerfen	(keine)
	TUC_KON_058	Displaygröße ermitteln	(keine)
Kartendienst	TUC_KON_005	Card-to-Card authentisieren	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD, FIA_UAU.5/AK, FMT_MTD.1.1/AK.Zert, FMT_MTD.1/AK.Zert
	TUC_KON_006	Datenzugriffsaudit eGK schreiben	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_012	PIN verifizieren	FDP_ACC.1/AK.PIN, FDP_ACF.1/AK.PIN
	TUC_KON_018	eGK-Sperrung prüfen	FPT_TEE.1/AK
	TUC_KON_019	PIN ändern	(keine)
	TUC_KON_021	PIN entsperren	(keine)
	TUC_KON_024	Karte zurücksetzen	(keine)
	TUC_KON_026	Liefere CardSession	FDP_ACC.1/AK.Infomod, FDP_ACC.1/AK.KD, FDP_ACF.1/AK.Infomod, FDP_ACF.1/AK.KD
	TUC_KON_027	PIN-Schutz ein-/ausschalten	(keine)
	TUC_KON_036	Liefere Fachliche Rolle	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_200	SendeAPDU	(keine)
	TUC_KON_202	Lese Datei	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_203	Schreibe Datei	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_204	Lösche Datei Inhalt	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_209	Lese Record	(keine)
	TUC_KON_210	Schreibe Record	(keine)
	TUC_KON_211	Lösche Record Inhalt	(keine)
	TUC_KON_214	Füge Hinzu Record	(keine)
	TUC_KON_215	Suche Record	(keine)
	TUC_KON_216	Lese Zertifikat	(keine)
	TUC_KON_218	Signiere	(keine)
	TUC_KON_219	Entschlüssele	(keine)
Systeminformationsdienst	TUC_KON_252	Liefere KT_Liste	(keine)
	TUC_KON_253	Liefere Karten_Liste	(keine)
	TUC_KON_254	Liefere Ressourcendetails	FDP_ACC.1/AK.Infomod, FDP_ACF.1/AK.Infomod

SFR-Zuordnung der TUCs für Fachmodule

Basisdienst	TUC	Beschreibung	SFR
	TUC_KON_256	Systemereignis absetzen	(keine)
Verschlüsselungsdienst	TUC_KON_070	Daten hybrid verschlüsseln	(keine)
	TUC_KON_071	Daten hybrid entschlüsseln	(keine)
	TUC_KON_072	Daten symmetrisch verschlüsseln	FCS_COP.1/AK.AES, FCS_COP.1/AK.CMS.Ver, FCS_COP.1/AK.XML.Ver, FDP_ETC.2/AK.Enc
	TUC_KON_073	Daten symmetrisch entschlüsseln	(keine)
	TUC_KON_075	Symmetrisch verschlüsseln	FCS_COP.1/AK.AES, FCS_COP.1/AK.CMS.Ver, FCS_COP.1/AK.XML.Ver, FDP_ETC.2/AK.Enc
	TUC_KON_076	Symmetrisch entschlüsseln	FCS_COP.1/AK.AES, FCS_COP.1/AK.CMS.Ent, FCS_COP.1/AK.XML.Ent, FDP_ITC.2/AK.Enc
Signaturdienst	TUC_KON_150	Dokument QES signieren	(keine)
	TUC_KON_151	QES-Dokumentensignatur prüfen	FDP_ACC.1/AK.SigPr, FDP_ACF.1/AK.SigPr, FDP_DAU.2/AK.QES
	TUC_KON_158	Komfortsignaturen erstellen	FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK
	TUC_KON_160	Dokumente nonQES signieren	FCS_COP.1/AK.CMS.Sign, FCS_COP.1/AK.PDF.Sign, FCS_COP.1/AK.XML.Sign
	TUC_KON_162	Kryptographische Prüfung der XML-Dokumentensignatur	FCS_COP.1/AK.XML.SigPr
	TUC_KON_170	Dokumente mit Komfort signieren	FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK
	TUC_KON_171	Komfortsignatur einschalten	FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK
	TUC_KON_172	Komfortsignatur ausschalten	FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK
	TUC_KON_173	Liefere Signaturmodus	FDP_ACF.1/AK.Sgen, FMT_MSA.4/AK
Zertifikatsdienst	TUC_KON_034	Zertifikatsinformationen extrahieren	FDP_ACC.1/AK.KD, FDP_ACF.1/AK.KD
	TUC_KON_037	Zertifikat prüfen	FPT_TDC.1/AK, FPT_TDC.1/NK.TLS.Zert, FPT_TDC.1/NK.Zert, FPT_TDC.1/SGD.Zert, FPT_TDC.1/VAU.Zert
	TUC_KON_042	CV-Zertifikat prüfen	(keine)
TLS-Dienst	TUC_KON_110	TLS-Verbindung aufbauen (kartenbas.)	FDP_ACC.1/AK.TLS, FDP_ACF.1/AK.TLS
	TUC_KON_111	Kartenbasierte TLS-Verbindung abbauen	(keine)
LDAP-Proxy	TUC_KON_290	LDAP-Verbindung aufbauen	(keine)
	TUC_KON_291	Verzeichnis abfragen	(keine)
	TUC_KON_292	LDAP-Verbindung trennen	(keine)
	TUC_KON_293	Verzeichnisabfrage abbrechen	(keine)
Protokollierungsdienst	TUC_KON_271	Schreibe Protokolleintrag	FAU_GEN.1/NK.SecLog
Namensdienst	TUC_KON_361	DNS-Namen auflösen	(keine)
	TUC_KON_362	Liste der Dienste abrufen	(keine)
	TUC_KON_363	Dienstdetails abrufen	(keine)

SFR-Zuordnung der TUCs für Fachmodule

Basisdienst	TUC	Beschreibung	SFR
Zeitdienst	TUC_KON_351	Liefere Systemzeit	FPT_STM.1/AK, FPT_STM.1/NK
StorageService	—	—	FDP_ACC.1/AK.SDS, FDP_ACF.1/AK.SDS
Benachricht.-dienst	—	—	
VAU-Service	—	—	FCS_CKM.1/VAU, FCS_COP.1/VAU.ECDSA, FCS_COP.1/VAU.AES, FCS_COP.1/VAU.Hash, FPT_TDC.1/VAU.Zert, FTP_ITC.1/VAU
SGD-Service	—	—	FCS_COP.1/SGD.ECDSA, FCS_COP.1/SGD.ECIES, FCS_COP.1/SGD.Hash, FTP_ITC.1/SGD, FDP_ITC.2/SGD, FDP_ACC.1/SGD, FDP_ACF.1/SGD, FPT_TDC.1/SGD.Zert

Tabelle 8.1.: SFR-Zuordnung der TUCs für Fachmodule

Die gematik Spezifikation für den Konnektor [gemSpec_Kon] regelt, welche TUCs der Basiskonnektor den Fachmodulen zur Verfügung stellen muss. Tabelle 8.2 führt diese TUCs auf und bildet sie auf die Funktionen der Schnittstelle LS.FM.RMI ab. Die Tabelle listet ebenfalls auf, welches Fachmodul welche API-Funktion nutzt.

Anmerkungen zur Tabelle

Folgende Punkte müssen bei der Interpretation der Tabelle in Betracht gezogen werden.

- Nicht alle von der Spezifikation genannnten TUCs werden in der gegenwärtigen Version des Konnektors für die Fachmodule angeboten. TUCs, bei denen die Felder „Java-Interface“ und „Methode“ nicht befüllt sind („—“), können nicht von den Fachmodulen aufgerufen werden.
- Über die von der Spezifikation geforderten TUCs hinaus gibt es Funktionen, die Fachmodule am Basiskonnektor aufrufen können. Solche Funktionen sind in der Spalte „TUC“ mit „—“ gekennzeichnet.
- Die Interfaces liegen im Package `de.koco.konnektor.ndesign.rmi.api`.
- Die Tabelle bildet lediglich die TUCs auf Methodenaufrufe ab. Die Aufrufparameter der Java-Interfaces sind in der API dokumentiert.

Basisdienst	TUC	Name des TUC	Interface	Methode	*NFDM*	*AMTS*	*ePA*
Zugriffsberechtigungsdienst	TUC_KON_000	Prüfe Zugriffsberechtigung	IAccessAuthorizatonServiceRemote	checkAccessAuthorization()	✓	✓	✓
Dienstverzeichnisdienst	TUC_KON_041	Einbringen der Endpunktinformationen während der Bootup-Phase	IFachmodulRegistrationRemote	registerFM()	✓	✓	✓
Kartenterminaldienst	TUC_KON_051	Mit Anwender über Kartenterminal interagieren	ICardTerminalInfoServiceRemote	interact()	✓	✓	✓
	TUC_KON_056	Karte anfordern	CardTerminalServiceInternRemote	karteAnfordern()	.	.	.
	TUC_KON_057	Karte auswerfen	CardTerminalServiceInternRemote	karteAuswerfen()	.	.	.
	TUC_KON_058	Displaygröße ermitteln	ICardTerminalInfoServiceRemote	getDisplayCapabilities()	.	.	✓
Kartendienst	TUC_KON_005	Card-to-Card authentisieren	ICardServiceRemote	cardToCard()	✓	✓	✓
	TUC_KON_006	Datenzugriffsaudit eGK schreiben	ICardServiceRemote	writeAccessAudit()	✓	✓	.
	TUC_KON_012	PIN verifizieren	ICardServiceRemote	verifyPin()	✓	✓	✓
	TUC_KON_018	eGK-Sperrung prüfen	ICardServiceRemote	checkEGKLock()	✓	✓	✓
	TUC_KON_019	PIN ändern	ICardServiceRemote	changePin()	.	.	.
	TUC_KON_021	PIN entsperren	ICardServiceRemote	unblockPin()	.	.	.
	TUC_KON_022	Liefere PIN-Status	ICardServiceRemote	getPinStatus()	✓	✓	✓
	TUC_KON_023	Karte reservieren	ICardServiceRemote	reserveCard()	✓	✓	✓
	TUC_KON_024	Karte zurücksetzen	ICardServiceRemote	resetCard()	.	.	.
	TUC_KON_026	Liefere CardSession	ICardServiceRemote	deliverCardSession()	✓	✓	✓
	TUC_KON_027	PIN-Schutz ein-/ausschalten	ICardServiceRemote	toggleVerificationRequirement()	.	.	.
	TUC_KON_036	Liefere Fachliche Rolle	ICardServiceRemote	getProfessions()	.	✓	✓
	TUC_KON_200	SendeAPDU	ICardServiceRemote	sendAPDU()	.	.	.
	TUC_KON_202	Lese Datei	ICardServiceRemote	readFile()	✓	✓	.
	TUC_KON_203	Schreibe Datei	ICardServiceRemote	writeFile()	✓	✓	.
	TUC_KON_204	Lösche Datei Inhalt	ICardServiceRemote	deleteFileContent()	✓	✓	.
	TUC_KON_209	Lese Record	ICardServiceRemote	readRecord()	.	.	.
	TUC_KON_210	Schreibe Record	ICardServiceRemote	writeRecord()	.	.	.
	TUC_KON_211	Lösche Record Inhalt	ICardServiceRemote	eraseRecord()	.	.	.
	TUC_KON_214	Füge Hinzu Record	ICardServiceRemote	addRecord()	.	.	.
	TUC_KON_215	Suche Record	ICardServiceRemote	searchRecord()	.	.	.
	TUC_KON_216	Lese Zertifikat	ICardServiceRemote	readCertificate()	.	.	✓
	TUC_KON_218	Signiere	ICardServiceRemote	signPKCS1V15()	.	.	.
	TUC_KON_219	Entschlüssele	ICardServiceRemote	decrypt()	.	.	.
Systeminform.-dienst	TUC_KON_252	Liefere KT_Liste	ISystemInformationServiceRemote	getCardTerminalsFacade()	.	.	.

Funktionen des Basiskonnektors für die Fachmodule

Basisdienst	TUC	Name des TUC	Interface	Methode	*NFDM*	*AMTS*	*ePA*
	TUC_KON_253	Liefere Karten_Liste	ISystemInformationServiceRemote	getCardsFacade()	.	.	✓
	TUC_KON_254	Liefere Ressourcendetails	ISystemInformationServiceRemote	getResourceInformationFacade()	✓	✓	✓
	TUC_KON_254	Liefere Ressourcendetails	ISystemInformationServiceRemote	getResourceInformationFacadeEGK()	✓	✓	✓
	TUC_KON_254	Liefere Ressourcendetails	ISystemInformationServiceRemote	getResourceInformationFacadeHPC()	.	.	.
	TUC_KON_256	Systemereignis absetzen	INotificationRemote	notify()	.	.	.
Verschlüsselungsdienst	TUC_KON_070	Daten hybrid verschlüsseln	IEncryptionServiceRemote	encryptDocument()	.	.	.
	TUC_KON_071	Daten hybrid entschlüsseln	IEncryptionServiceRemote	decryptDocument()	.	.	.
	TUC_KON_072	Daten symmetrisch verschlüsseln	IEncryptionServiceRemote	encryptDocument()	.	.	✓
	TUC_KON_073	Daten symmetrisch entschlüsseln	IEncryptionServiceRemote	decryptDocument()	.	.	.
	TUC_KON_075	Symmetrisch verschlüsseln	IEncryptionServiceRemote	encrypt()	.	.	✓
	TUC_KON_075	Symmetrisch verschlüsseln	IEncryptionServiceRemote	encryptDocument()	.	.	.
	TUC_KON_075	Symmetrisch verschlüsseln	IEncryptionServiceRemote	encryptXMLEncryptedData()	.	.	✓
	TUC_KON_076	Symmetrisch entschlüsseln	IEncryptionServiceRemote	decrypt()	.	.	✓
	TUC_KON_076	Symmetrisch entschlüsseln	IEncryptionServiceRemote	decryptXMLEncryptedData()	.	.	✓
	—	—	IEncryptionServiceRemote	generateSymmetricKey()	.	.	✓
Signaturdienst	TUC_KON_150	Dokument QES signieren	ISignserviceRemote	signQESDocument()†	.	.	.
	TUC_KON_151	QES-Dokumentensignatur prüfen	ISignserviceRemote	verifyDocument()†	✓	.	.
	TUC_KON_158	Komfortsignaturen erstellen	—	—	.	.	.
	TUC_KON_160	Dokumente nonQES signieren	ISignserviceRemote	signNonQESDocument()†	.	.	.
	TUC_KON_160	Dokumente nonQES signieren	ISignserviceRemote	signAssertionDocument()‡	.	.	✓
	TUC_KON_162	Kryptographische Prüfung der XML-Dokumentensignatur	ISignserviceRemote	verifyXMLDocumentSignature()†	✓	.	.
	TUC_KON_170	Dokumente mit Komfort signieren	—	—	.	.	.
	TUC_KON_171	Komfortsignatur einschalten	—	—	.	.	.
	TUC_KON_172	Komfortsignatur ausschalten	—	—	.	.	.
	TUC_KON_173	Liefere Signaturmodus	—	—	.	.	.
Zertifikatsdienst	TUC_KON_034	Zertifikatsinformationen extrahieren	ICertificateServiceRemote	extractCertificateInformation()	✓	✓	.
	TUC_KON_037	Zertifikat prüfen	ICertificateServiceRemote	verifyCertificateX509NonQES()	.	.	.
	TUC_KON_037	Zertifikat prüfen	ICertificateServiceQESRemote	verifyCertificateX509QES()	.	.	.
TLS-Dienst	TUC_KON_110	TLS-Verbindung aufbauen (kartenbas.)	ITlsServiceRemote	createTlsConnection()	.	.	✓
	TUC_KON_111	Kartenbasierte TLS-Verbindung abbauen	—	—	.	.	.

Funktionen des Basiskonnektors für die Fachmodule

Basisdienst	TUC	Name des TUC	Interface	Methode	*NFDM*	*AMTS*	*ePA*
LDAP-Proxy	TUC_KON_290	LDAP-Verbindung aufbauen	—	—	.	.	.
	TUC_KON_291	Verzeichnis abfragen	—	—	.	.	.
	TUC_KON_292	LDAP-Verbindung trennen	—	—	.	.	.
	TUC_KON_293	Verzeichnisabfrage abbrechen	—	—	.	.	.
Protokollierungsdienst	TUC_KON_271	Schreibe Protokolleintrag	ILoggingServiceRemote	log()	✓	✓	✓
	—	Auslesen der Log-Konfiguration	ILoggingServiceRemote	getConfiguration()	✓	✓	✓
	—	Schreiben der Log-Konfiguration	ILoggingServiceRemote	setConfiguration()	✓	✓	✓
Namensdienst	TUC_KON_361	DNS-Namen auflösen	IDNSServiceRemote	resolveFQDN()	.	.	✓
	TUC_KON_362	Liste der Dienste abrufen	IDNSServiceRemote	listServiceNames()	.	.	✓
	TUC_KON_363	Dienstdetails abrufen	IDNSServiceRemote	listServiceDetails()	.	.	✓
	—	DNS Toplevel Domain abrufen	IDNSServiceRemote	getTopLevelDomainName()	.	.	✓
Zeitdienst	TUC_KON_351	Liefere Systemzeit	INTPServiceRemote	getSystemTime()	✓	✓	✓
StorageService	—	Löschen einer Datei	IStorageServiceRemote	deleteFile()	.	.	.
	—	Verzeichnis lesen	IStorageServiceRemote	listFiles()	.	.	.
	—	Datei lesen	IStorageServiceRemote	loadFile()	.	.	✓
	—	Datei speichern	IStorageServiceRemote	storeFile()	.	.	✓
Benachricht.-dienst	—	Versenden eines Events an den AK	IEventhandlerNotifierRemote	notify()	.	.	✓
	—	EventHandler registrieren	IEventHandlerRegistrarRemote	registerEventHandler()	✓	✓	✓
	—	EventHandler deregistrieren	IEventHandlerRegistrarRemote	unregisterEventHandler()	.	.	.
VAU-Service	—	VAU Verbindung anfordern	IVAUServiceRemote	getVauChannel()	.	.	✓
	—	VAU Verbindung öffnen	IVAUServiceRemote	openChannel()	.	.	✓
	—	Status abfragen	IVAUServiceRemote	status()	.	.	✓
	—	VAU Verbindung schließen	IVAUServiceRemote	closeChannel()	.	.	✓
	—	VAU Verbindung freigeben	IVAUServiceRemote	freeChannel()[×]	.	.	✓
SGD-Service	—	Berechtigtenschlüssel ableiten	ISGDServiceRemote	deriveKey()	.	.	✓

[✓] Methode wird von Fachmodul genutzt.
[†] Nur für Signaturen zu verwenden, die gemäß Security Target zugelassen sind.
[‡] Nur für SAML2-Assertions gemäß ePA Spezifikation [gemSpec_FM_ePA] zu verwenden.
[×] Das Fachmodul ePA muss diese Methode aufrufen, wenn die fachliche Bearbeitung beendet ist.

Tabelle 8.2.: Funktionen des Basiskonnektors für die Fachmodule

A. Erklärung der tabellarischen Darstellung

Tabelle A.1 zeigt die in den Tabellen dieses Dokuments verwendeten Symbole. Diese kommen in allen Tabellen zum Einsatz, in denen Entitäten der Common Criteria aufeinander abgebildet werden.

Symbol	Beschreibung
.	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 Kartenterminal	CardService::de.ndesign.koco.ifd.sicct	4742	SMC-KT: ID.SMKT.AUT	CertificateService::Core
TLS.7	LS.WAN.RegService	Client	✓	Registrierungsdienst	AdminService::RegistrationService	8443	C.ZD.TLS-S, 1.2.276.0.76.4.157	CertificateService::Core
TLS.8	LS.VPN_TI.LDAP	Client	.	Verzeichnisdienst	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

C. Composition Requirements für Fachmodule

Fachmodule unterliegen im Konnektor Restriktionen und Auflagen. Diese werden in der Konnektor Security Guidance beschrieben [AGD_Kon-Sec]. Die dort beschriebenen Composition Requirements müssen vom Entwickler eines Fachmoduls eingehalten werden, um die Funktionsfähigkeit des Gesamtkonnektors nicht zu gefährden. Zur besseren Lesbarkeit werden die Composition Requirements hier wiederholt[1]. Einen präziseren Einblick mit mehr Erklärungen liefert die Konnektor Security Guidance.

COMP-REQ-1 Korrekte Benutzung des Konnektors

Das Fachmodul MUSS den Basiskonnektor entsprechend der vorliegenden Dokumentation und der Spezifikation der gematik benutzen. Das Fachmodul DARF NICHT die Sicherheitsfunktionen des Konnektors beeinträchtigen oder missbrauchen.

COMP-REQ-2 Auslieferungsformat

Das Fachmodul MUSS als Web-Anwendung entwickelt und als Web Application Archive ausgeliefert werden.

COMP-REQ-3 Registrierung am Basiskonnektor

Das Fachmodul MUSS sich gemäß TUC_KON_041 mit `IFachmodulRegistrationRemote.registerFM()` am Basiskonnektor registrieren.

COMP-REQ-4 Signaturrichtlinien

Das Fachmodul KANN während der Registrierung eigene Signaturrichtlinien in den Basiskonnektor einbringen. Das Fachmodul DARF NICHT andere Signaturrichtlinien verwenden. Das Fachmodul DARF NICHT Signaturrichtlinien oder Signaturvarianten verwenden, die über Tabelle 7.1 des Security Targets hinausgehen.

COMP-REQ-5 Aufrufe des Basiskonnektors

Das Fachmodul KANN die in Tabelle 8.2 angegebenen Aufrufe des Basiskonnektors verwenden. Dabei MUSS es sich mit seinem Token authentisieren. Das Fachmodul MUSS die Schnittstelle LS.FM.RMI gemäß der Dokumentation der Java-API verwenden. Das Fachmodul DARF NICHT andere Funktionen des Basiskonnektors aufrufen.

COMP-REQ-6 Separation der Bibliotheken

Das Fachmodul MUSS Bibliotheken aus seinem eigenen Class-Loader verwenden. Es DARF NICHT auf die Bibliotheken und Klassen im Class-Loader anderer Fachmodule zugreifen.

COMP-REQ-7 Konfigurationsparameter für Logging

Das Fachmodul KANN während der Registrierung Konfigurationsfelder für Loggingparameter an den Basiskonnektor übergeben.

[1] Referenzen werden angepasst, um auf das Security Target statt auf die Konnektor Security Guidance zu verweisen.

Das Fachmodul MUSS die Konfigurationsparameter mit der Funktion `ILoggingServiceRemote.setConfiguration()` des Basiskonnektors persistieren.

COMP-REQ-8 Konfigurationsparameter

Das Fachmodul KANN während der Registrierung Konfigurationsfelder für Konfigurationsparameter an den Basiskonnektor übergeben.

Vom Basiskonnektor an das Fachmodul übergebene Konfigurationswerte MUSS das Fachmodul gemäß den Vorgaben der entsprechenden Spezifikation prüfen. Das Fachmodul MUSS die geprüften Konfigurationsparameter mit Funktionsaufrufen des Basiskonnektors persistieren.

COMP-REQ-9 Protokollierung

Das Fachmodul KANN Meldungen in das Fachmodulprotokoll des Konnektors schreiben. Dafür MUSS sich das Fachmodul beim Basiskonnektor authentisieren.

COMP-REQ-10 gematik Schnittstellendefinitionen

Das Fachmodul KANN die Schnittstellendefinitionsdateien der gematik, die der Basiskonnektor bereitstellt, verwenden.

COMP-REQ-11 Keine Außenschnittstellen

Das Fachmodul DARF NICHT eigene Außenschnittstellen anbieten. Es MUSS zur Kommunktion mit den Clientsystemen SOAP-Verbindungen nutzen, die vom Proxy-Server des Basiskonnektors vermittelt werden.

COMP-REQ-12 Validierung der Eingabedaten

Das Fachmodul MUSS die vom Basiskonnektor übergebenen Eingabedaten selbst prüfen und validieren, um sich vor Angriffen von Clientsystemen zu schützen.

COMP-REQ-13 Verbindungen zu Drittsystemen

Das Fachmodul DARF NICHT unkontrollierte Verbindungen zu Drittsystemen aufbauen.

D. Anforderungen zur sicherheitstechnischen Eignung

In Abschnitt 3.2.1 des *Produkttypsteckbrief Konnektor* listet die gematik Anforderungen zur sicherheitstechnischen Eignung des Konnektors auf, die durch die CC-Evaluierung abgedeckt werden müssen [gemProdT_Kon_PTV5P].

Die gematik fordert den Hersteller dazu auf, die Teile des Security Targets zu markieren, bei denen das Security Target die Anforderungen der Schutzprofile [BSI-CC-PP-0097; BSI-CC-PP-0098] erweitert. Diese Erweiterungen sind notwendig, da das Schutzprofil nicht alle Anforderungen der gematik Spezifikation abdeckt. Ausgangspunkt für die Erweiterungen ist Produkttypsteckbrief PTV2 [gemProdT_Kon_PTV2]. In dieser Produkttypversion waren alle Anforderungen durch das Schutzprofil abgedeckt. In den folgenden Produkttypversionen muss der Hersteller die Erweiterungen selbst vornehmen. Tabelle D.1 zeigt die seit PTV2 hinzugekommenen Anforderungen sowie deren Abdeckung durch SFR in diesem Security Target.

Hinweis zu aktualisierten Anforderungen aus PTV2

In neueren Produkttypsteckbriefen sind einige Anforderungen gegenüber PTV2 aktualisiert. Diese tragen ein Suffix in der Form „-01“. Für diese neuen Versionen der Anforderungen aus PTV2 gelten in diesem Verfahren *dieselben* Abdeckungen durch SFR wie für die ursprünglichen Versionen aus PTV2. Die inhaltlichen Anpassungen der Anforderungen in neueren Produkttypversionen machen keine Neumodellierung durch SFR erforderlich. Solche Anforderungen sind in der Tabelle mit „Abdeckung identisch zu <*afo*> aus PTV2“ gekennzeichnet. Die Zuordnung „(Kein SFR)“ ist technisch bedingt, es gilt dieselbe Zuordnung, die PTV2 bereits angenommen hat.

Afo	SFR		Mapping	Spezifikation
A_14223	FPT_TDC.1/NK.TLS.Zert	Refinement (2) an FPT_TDC.1.2/NK.TLS.Zert	ST	[gemSpec_FM_ePA]
A_14930	FPT_TDC.1/NK.TLS.Zert	Refinement (2) an FPT_TDC.1.2/NK.TLS.Zert	ST	[gemSpec_FM_ePA]
A_15210	FPT_TDC.1/VAU.Zert	Refinement an FPT_TDC.1.2/VAU.Zert(2)	ST	[gemSpec_FM_ePA]
A_15532	FPT_TDC.1/NK.TLS.Zert	Refinement (2) an FPT_TDC.1.2/NK.TLS.Zert	ST	[gemSpec_FM_ePA]
A_15549	FCS_CKM.1/VAU FCS_COP.1/VAU.AES FCS_COP.1/VAU.Hash FTP_ITC.1/VAU	Brainpool p256r1 für VAU AES256-GCM für VAU SHA-256 für VAU Schlüsselvernichtung nach 24h für VAU	ST	[gemSpec_Krypt]
A_15561	(Kein SFR)	Keine AES-NI Unterstützung im TOE	ST	[gemSpec_Krypt]
A_16203	FPT_FLS.1/AK	Auslösen des kritischen Betriebszustands bei *EC_Firewall_Not_Reliable* gemäß TIP1-A_4510-05	ST	[gemSpec_Kon]
A_16849	FCS_CKM.4/AK FDP_RIP.1/AK	Sicheres Löschen durch Garbage Collection Sicheres Löschen durch Garbage Collection	ST	[gemSpec_Krypt]
A_16852-01	FCS_CKM.1/VAU	Schlüsselableitung mit ECDH	ST	[gemSpec_Krypt]
A_16883-01	FCS_CKM.1/VAU FCS_COP.1/VAU.Hash	Generieren des ephemeren Schlüssels Hashberechnung über Zertifikat und VAUClientHello	ST	[gemSpec_Krypt]
A_16884	FTP_ITC.1/VAU	Refinements am SFR-Text fordern Protokollkonformität	ST	[gemSpec_Krypt]
A_16897	FTP_ITC.1/VAU	Protokollablauf / Versand ClientHello	ST	[gemSpec_Krypt]
A_16899	FTP_ITC.1/VAU	Protokollablauf / Prüfung VAUServerSigFin	ST	[gemSpec_Krypt]
A_16900	FTP_ITC.1/VAU	Abbruch nach Server-Fehlermeldung	ST	[gemSpec_Krypt]
A_16903	FCS_COP.1/VAU.Hash FTP_ITC.1/VAU	Hash-Berechnung Protokollablauf / Hash-Berechnung	ST	[gemSpec_Krypt]
A_16941-01	FTP_ITC.1/VAU	Protokollablauf / Signaturprüfung	ST	[gemSpec_Krypt]
A_16943-01	FCS_CKM.1/VAU	Schlüsselableitung	ST	[gemSpec_Krypt]

Afo	SFR		Mapping	Spezifikation
A_16945-02	FCS_COP.1/VAU.AES FTP_ITC.1/VAU FTP_ITC.1/VAU	Authenticated Data Protokollablauf / Authenticated Data Protokollablauf / Nutzerdatentransport	ST	[gemSpec_Krypt]
A_16957-01	FTP_ITC.1/VAU FTP_ITC.1/VAU	Protokollablauf / Fehlerbehandlung Protokollablauf / Zählerwerte	ST	[gemSpec_Krypt]
A_16958	FTP_ITC.1/VAU	Protokollablauf / Schlüsselaushandlung	ST	[gemSpec_Krypt]
A_17069	FTP_ITC.1/VAU	Protokollablauf / Zählerüberlauf	ST	[gemSpec_Krypt]
A_17070-02	FCS_COP.1/VAU.Hash FTP_ITC.1/VAU	Hashberechnung VAUClientSigFin Protokollablauf / VAUClientSigFin	ST	[gemSpec_Krypt]
A_17071	FTP_ITC.1/VAU	Protokollablauf / VAUClientSigFin	ST	[gemSpec_Krypt]
A_17074	FTP_ITC.1/VAU	Protokollablauf / Ignoriere unbekannte Datenfelder	ST	[gemSpec_Krypt]
A_17081	(Kein SFR) FPT_TDC.1/VAU.Zert	Signatur erfolgt durch Karte in der Umgebung Serverzertifikat prüfen	ST	[gemSpec_Krypt]
A_17084	FCS_COP.1/VAU.Hash FTP_ITC.1/VAU	Prüfung Hash in VAUServerSigFin Protokollablauf / Prüfung VAUServerSigFin	ST	[gemSpec_Krypt]
A_17094-01	FCS_CKM.1/NK.TLS FTP_ITC.1/NK.TLS	Erweiterung des Refinements zu FTP_ITC.1/NK.TLS Erweiterung des Refinements zu FTP_ITC.1/NK.TLS	ST	[gemSpec_Krypt]
A_17124-01	FCS_CKM.1/NK.TLS FTP_ITC.1/NK.TLS FCS_CKM.1/NK.Zert	Erweiterung des Refinements zu FCS_CKM.1/NK.TLS Erweiterung des Refinements zu FTP_ITC.1/NK.TLS Erweiterung des Refinements zu FCS_CKM.1/NK.Zert	ST	[gemSpec_Krypt]
A_17125	FCS_COP.1/NK.Auth	IPsec Signaturprüfung und -erstellung mit ECDSA	ST	[gemSpec_Krypt]
A_17205	FCS_COP.1/AK.Sig-Ver.ECDSA FCS_COP.1/NK.SigVer	TSL-Signaturprüfung ECDSA Algorithmen für die TSL-Signaturprüfung	ST	[gemSpec_Krypt]

Afo	SFR		Mapping	Spezifikation
A_17206	FCS_COP.1/AK.Sig-Ver.ECDSA	XML-Signaturprüfung ECDSA	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.XML.Sign	XML-Signaturerstellung ECDSA		
	FCS_COP.1/AK.XML.SigPr	XML-Signaturprüfung ECDSA		
A_17207	FCS_COP.1/AK.CMS.Sign	CMS-Signaturerstellung ECDSA	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.CMS.SigPr	CMS-Signaturprüfung ECDSA		
A_17208	FCS_COP.1/AK.PDF.Sign	PDF-Signaturerstellung ECDSA	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.PDF.SigPr	PDF-Signaturprüfung ECDSA		
A_17209	FCS_COP.1/AK.CMS.Sign	Binärstring signieren für External Authentication	ST	[gemSpec_Krypt]
A_17210	(Kein SFR)	Wird vom TOE in PTV 5+ nicht umgesetzt.	ST	[gemSpec_Krypt]
A_17220	FCS_COP.1/AK.CMS.Ent	ECIES-Entschlüsselung für binäre Daten	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.CMS.Ver	ECIES-Verschlüsselung für binäre Daten		
	FCS_COP.1/AK.ECIES	Ablauf der ECIES-Verschlüsselung		
A_17221-01	(Kein SFR)	Wird vom TOE in PTV 5+ nicht umgesetzt.	ST	[gemSpec_Krypt]
A_17225-01	FPT_TDC.1/VAU.Zert	Prüfung der Eigenschaften in FPT_TDC.1.2/VAU.Zert(2)	ST	[gemSpec_Kon]
A_17322	FTP_ITC.1/NK.TLS	Refinement schließt nicht-genannte Ciper Suiten aus.	ST	[gemSpec_Krypt]
A_17359	FCS_COP.1/AK.CMS.Sign	CMS-Signaturerstellung ECDSA	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.CMS.SigPr	CMS-Signaturprüfung ECDSA		
A_17360	FCS_COP.1/AK.Sig-Ver.ECDSA	XML-Signaturprüfung ECDSA	ST	[gemSpec_Krypt]
	FCS_COP.1/AK.XML.Sign	XML-Signaturerstellung ECDSA		
	FCS_COP.1/AK.XML.SigPr	XML-Signaturprüfung ECDSA		
A_17548-01	FPT_TST.1/AK.Run-time	FPT_TST.1.2/AK.Run-time fordert Prüfung der Integrität der TSF-Konfigurationsdaten. TSL gehört zu den TSF-Konfigurationsdaten. Die Integrität der TSF-Konfiguration entsteht durch den sicheren Speicher. Also liegt die TSL im sicheren Speicher.	ST	[gemSpec_Kon]

Afo	SFR		Mapping	Spezifikation
A_17549-01	FPT_TDC.1/AK	Signaturprüfung TSL und TSL-Signer-CA Cross-Zertifikat, ST-Anwendungshinweis zu FPT_TDC.1.1/AK(6)	ST	[gemSpec_Kon]
A_17661	FTP_ITC.1/AK.TSL	Refinement an FTP_ITC.1.3/AK.TSL	ST	[gemSpec_Kon]
A_17688	FPT_TDC.1.1/AK	Nutzung der TSL(ECC-RSA)	ST	[gemSpec_PKI]
A_17690	FTP_ITC.1/AK.TSL	Refinement an FTP_ITC.1.3/AK.TSL	ST	[gemSpec_PKI]
A_17746	FCS_COP.1/AK.CMS.Ent FCS_COP.1/AK.CMS.Ver	Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials	ST	[gemSpec_Kon]
A_17768	FCS_COP.1/AK.CMS.Sign FCS_COP.1/AK.CMS.SigPr FCS_COP.1/AK.PDF.Sign FCS_COP.1/AK.PDF.SigPr FCS_COP.1/AK.XML.Sign FCS_COP.1/AK.XML.SigPr	Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials Auswahl des korrekten Schlüsselmaterials	ST	[gemSpec_Kon]
A_17777	FCS_COP.1/SGD.ECDSA FCS_COP.1/SGD.ECIES FCS_COP.1/SGD.ECIES FCS_COP.1/SGD.ECIES FCS_COP.1/SGD.ECIES FCS_COP.1/SGD.Hash	A_17874 in [gemSpec_Krypt, Kap. 3.15.5] A_17872 in [gemSpec_Krypt, Kap. 3.15.5] A_17874 in [gemSpec_Krypt, Kap. 3.15.5] A_17875 (2) in [gemSpec_Krypt, Kap. 3.15.5] A_17875 (3) in [gemSpec_Krypt, Kap. 3.15.5] A_17875 (3) in [gemSpec_Krypt, Kap. 3.15.5]	ST	[gemSpec_Kon]
A_17821	FPT_TDC.1.2/NK.Zert	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA	ST	[gemSpec_PKI]
A_17837-01	FPT_TDC.1/NK.Zert	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA	ST	[gemSpec_Kon]
A_17847	FPT_TDC.1/SGD.Zert	Prüfkriterium in FPT_TDC.1.2/SGD.Zert(1)	ST	[gemSpec_SGD_ePA]
A_17848	FPT_TDC.1/SGD.Zert	Prüfkriterium in FPT_TDC.1.2/SGD.Zert(2)	ST	[gemSpec_SGD_ePA]

Afo	SFR		Mapping	Spezifikation
A_17874	FCS_COP.1/SGD.ECDSA	Authentisierung des öffentlichen ECIES-Schlüssels des Clients mit Karte (Umgebung)	ST	[gemSpec_Krypt]
	FCS_COP.1/SGD.ECIES	Verwendung Brainpool bei Schlüsselableitung		
	FCS_COP.1/SGD.ECIES	Verwendung von brainpoolP256r1 für eph. Schlüssel		
A_17875	FCS_COP.1/SGD.ECIES	HKDF / Unterpunkt (3)	ST	[gemSpec_Krypt]
	FCS_COP.1/SGD.ECIES	Schlüsselaustauch nach NIST-800-56-A / Unterpunkt (2)		
	FCS_COP.1/SGD.Hash	HKDF / Unterpunkt (3)		
A_17888	FTP_ITC.1/SGD	Protokollablauf	ST	[gemSpec_SGD_ePA]
A_17889	FTP_ITC.1/SGD	Protokollablauf	ST	[gemSpec_SGD_ePA]
A_17892	FTP_ITC.1/SGD	Protokollablauf / Ignoriere unbekannte Datenfelder	ST	[gemSpec_SGD_ePA]
A_17893	FTP_ITC.1/SGD	Protokollablauf / Prüfe maximale Größe	ST	[gemSpec_SGD_ePA]
A_17894-01	FDP_ITC.2/SGD	Kodierung des öffentlichen ECIES-Schlüssels des SGD	ST	[gemSpec_SGD_ePA]
A_17895-01	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_17897	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_17898	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_17899	FDP_ACC.1/SGD	Import des öffentlichen ECIES-Schlüssels eines SGD-HSM	ST	[gemSpec_SGD_ePA]
	FDP_ACF.1/SGD	Import des öffentlichen ECIES-Schlüssels eines SGD-HSM		
	FDP_ITC.2/SGD	Import des öffentlichen ECIES-Schlüssels eines SGD-HSM		
A_17900	FCS_COP.1/SGD.Hash	Berechnen des Hashwertes des eigenen Schlüssels	ST	[gemSpec_SGD_ePA]
	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD		
A_17901	(Kein SFR)	Signatur durch SM-B in der Umgebung des TOE	ST	[gemSpec_SGD_ePA]
	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD		
A_17902	FCS_COP.1/SGD.ECIES	Schlüsselübertragung der EC-Koordinaten	ST	[gemSpec_SGD_ePA]
	FCS_COP.1/SGD.ECIES	Verschlüsselung der übertragenenen EC-Koordinaten		
	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD		

Afo	SFR		Mapping	Spezifikation
A_17903	FCS_COP.1/SGD.ECIES	Vom Sender erzeugter ECC-Punkt MUSS auf der gleichen elliptischen Kurve wie der Empfänger-ECC-Punkt liegen	ST	[gemSpec_SGD_ePA]
A_17924-01	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_17930	(Kein SFR)	Ist für den Konnektor eine Aufgabe des Fachmoduls, wird nicht durch den SGD-Client umgesetzt.	ST	[gemSpec_SGD_ePA]
A_18001	FCS_COP.1/AK.AES FDP_ETC.2/AK.Enc	S. Eintrag TUC_KON_075 in Tabelle 8.2 S. Eintrag TUC_KON_075 in Tabelle 8.2	ST	[gemSpec_Kon]
A_18002	FCS_COP.1/AK.AES FDP_ITC.2/AK.Enc	S. Eintrag TUC_KON_076 in Tabelle 8.2 S. Eintrag TUC_KON_076 in Tabelle 8.2	ST	[gemSpec_Kon]
A_18003	FTP_ITC.1/SGD	Schlüsselableitung - Telematik-ID in Ableitungsvektor einbringen.	ST	[gemSpec_SGD_ePA]
A_18004	FCS_COP.1/VAU.AES	Vgl. ST-Anwendungshinweis **??**	ST	[gemSpec_Krypt]
A_18005	FCS_CKM.4/AK	Nach Ende der Operation wird der Schlüssel aus dem Speicher entfernt	ST	[gemSpec_SGD_ePA]
A_18006	FTP_ITC.1/SGD	Schlüsselableitung - KVNR in Ableitungsvektor einbringen.	ST	[gemSpec_SGD_ePA]
A_18021	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18024	FCS_COP.1/SGD.ECDSA FDP_ACC.1/SGD FDP_ACF.1/SGD FDP_ITC.2/SGD FPT_TDC.1/SGD.Zert	Prüfung der Zertifikatssignatur Import des SGD-HSM ECIES-Public Key Import des SGD-HSM ECIES-Public Key Import des SGD-HSM ECIES-Public Key Prüfregeln für Zertifikat	ST	[gemSpec_SGD_ePA]
A_18025-01	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18028	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18029	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18031-01	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]

Afo	SFR		Mapping	Spezifikation
A_18032	FCS_COP.1/SGD.ECIES FTP_ITC.1/SGD	Erzeugung des kurzlebigen Schlüsselpaars Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18464	FMT_MOF.1/NK.TLS	Vgl. ST-Anwendungshinweis 17 zu FMT_MOF.1.1/NK.TLS(3)	ST	[gemSpec_Krypt]
A_18465-01	FTP_ITC.1/VAU	Protokollablauf / MTOM	ST	[gemSpec_Krypt]
A_18466-01	FTP_ITC.1/VAU	Protokollablauf / HTTP-Protokoll	ST	[gemSpec_Krypt]
A_18467	(Kein SFR)	Keine TLS v1.3 Unterstützung im TOE für PTV4	ST	[gemSpec_Krypt]
A_18624	(Kein SFR)	Keine ECC Unterstützung für IPSec/IKE im TOE für PTV4	ST	[gemSpec_Krypt]
A_18686-01	FDP_ACF.1/AK.Sgen	Deaktivieren der Komfortsignatur nach Ablauf Timer	ST	[gemSpec_Kon]
A_18756	(Kein SFR)	XAdES nonQES wird nicht unterstützt, Ausnahme gem. A_20478 für SAML2	ST	[gemSpec_Kon]
A_18987	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_18988	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_19000	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_19052-01	(Kein SFR)	Härtungen an XML-Parsern gemäß TAB_KON_775	ST	[gemSpec_Kon]
A_19100-01	FDP_ACF.1/AK.Sgen	Deaktivieren der Komfortsignatur nach Ablauf Zähler	ST	[gemSpec_Kon]
A_19101	FIA_UAU.5/AK	Hinweis auf Verantwortung des Clientsystems	ST	[gemSpec_Kon]
A_19102-04	FDP_ACF.1/AK.Sgen	Refinements an FDP_ACF.1.2/AK.Sgen(4)(g)-(i)	ST	[gemSpec_Kon]
A_19103-07	FDP_ACF.1/AK.Sgen	Refinements an FDP_ACF.1.2/AK.Sgen(4)(g)-(i)	ST	[gemSpec_Kon]
A_19104-04	FDP_ACF.1/AK.Sgen	Refinements an FDP_ACF.1.2/AK.Sgen(4)(g)-(i)	ST	[gemSpec_Kon]
A_19258	FTP_ITC.1/AK.QSEE	Sicherer Kanal für Komfortsignaturen	ST	[gemSpec_Kon]
A_19738	FMT_MTD.1/AK.Admin	Die Anforderung ist zu feingranular für die Subjekt-Definition des PP. Das PP kennt nur die Rolle „Administrator“.	ST	[gemSpec_Kon]

Afo	SFR		Mapping	Spezifikation
A_19971	FCS_COP.1/SGD.Hash	SGD verwendet ausschließlich SHA-256	ST	[gemSpec_Krypt]
A_20073-01	FIA_UAU.5/AK	Längenprüfung der User ID auf 128 Bit	ST	[gemSpec_Kon]
A_20074	FIA_UAU.5/AK	Prüfung der Eindeutigkeit der User ID über die letzten 1.000 Vorgänge	ST	[gemSpec_Kon]
A_20478	FCS_COP.1/AK.XML.Sign	XML-Signaturerstellung ECDSA	ST	[gemSpec_Kon]
A_20549	FTP_ITC.1/VAU	Protokollablauf / HTTP-Protokoll	ST	[gemSpec_Krypt]
A_20977	FTP_ITC.1/SGD	Protokollablauf gemäß Refinement in FTP_ITC.1/SGD	ST	[gemSpec_SGD_ePA]
A_21185	FPT_TDC.1/NK.Zert	Signaturprüfung gemäß Refinement in FPT_TDC.1/NK.Zert	ST	[gemSpec_Kon]
A_21275-01	FCS_COP.1/NK.TLS.Auth	Hash-Algorithmen als Refinement im SFR explizit aufgeführt	ST	[gemSpec_Krypt]
A_21697-01	FDP_ITC.2/NK.TLS	Zusätzliche Regel in FDP_ITC.2.5/NK.TLS(2)	ST	[gemSpec_Kon]
A_21698	FMT_MOF.1/NK.TLS	Zusätzliche Regel in FMT_MOF.1/NK.TLS, ST-Anwendungshinweis 19	ST	[gemSpec_Kon]
A_21699-02	FCS_CKM.1/NK.Auth	Zusätzliche Sicherheitsanforderung FCS_CKM.1/NK.Auth	ST	[gemSpec_Kon]
A_21701	FDP_ETC.2/NK.TLS	Zusätzliche Regel in FDP_ITC.2.4/NK.TLS(2)	ST	[gemSpec_Kon]
A_21702	FMT_MOF.1/NK.TLS	Zusätzliche Regel in FMT_MOF.1/NK.TLS, ST-Anwendungshinweis 19	ST	[gemSpec_Kon]
A_21749-03	FDP_ACC.1/AK.Update FDP_ACF.1/AK.Update	Zusätzliches Objekt in FDP_ACC.1/AK.Update Zusätzliche Regeln in FDP_ACF.1/AK.Update	ST	[gemF_LZV_gSMC-K]
A_21760-01	FMT_MOF.1/NK.TLS	Zusätzliche Regel in FMT_MOF.1/NK.TLS, ST-Anwendungshinweis 19	ST	[gemSpec_Kon]
A_21811-03	FCS_CKM.1/NK.Zert	Auswahl der Kurventypen	ST	[gemSpec_Kon]
A_21879	FDP_ITC.2/NK.TLS	Zusätzliches Assignment in FDP_ITC.2.5/NK.TLS	ST	[gemF_LZV_gSMC-K]
A_21888	(Kein SFR)	Hinweis in Unterunterabschnitt 7.3.1.2	ST	[gemSpec_Krypt]

Afo	SFR		Mapping	Spezifikation
A_22344	(Kein SFR)	Hinweis zu drei parallelen Sessions in SF.SignatureService	ST	[gemSpec_Kon]
A_22352	(Kein SFR)	Hinweis zu unabhängigen Timern für parallele Sessions in SF.SignatureService	ST	[gemSpec_Kon]
A_22458	FIA_UAU.5/AK	Vgl. ST-Anwendungshinweis 25	ST	[gemSpec_Krypt]
A_22459	(Kein SFR)	Hinweis zu unabhängigen Zählern für parallele Sessions in SF.SignatureService	ST	[gemSpec_Kon]
A_22494	(Kein SFR)	Im TOE noch nicht umgesetzt	ST	[gemSpec_SGD_ePA]
A_22497	(Kein SFR)	KANN-Anforderung im TOE nicht umgesetzt	ST	[gemSpec_SGD_ePA]
A_22673	(Kein SFR)	Hinweis in den Signaturrichtlinien in SF.SignatureService	ST	[gemSpec_Kon]
A_22923	(Kein SFR)	Hinweis in den Signaturrichtlinien in SF.SignatureService	ST	[gemSpec_Kon]
A_23226-01	FCS_CKM.1/NK.TLS	Gemäß ANFKON-609 sind die Suiten auch für andere Verbindungen als legacy KTs verwendbar.	ST	[gemSpec_Krypt]
GS-A_4376-02	(Kein SFR)	Abdeckung identisch zu GS-A_4376 aus PTV2	PP	[gemSpec_Krypt]
GS-A_4446-05	FPT_TDC.1/NK.TLS.Zert	Refinement FPT_TDC.1.2/NK.TLS.Zert(2)	ST	[gemSpec_OID]
GS-A_4651	FPT_TDC.1/VAU.Zert	Assignment FPT_TDC.1.2/VAU.Zert	ST	[gemSpec_PKI]
GS-A_4663	FPT_TDC.1/NK.TLS.Zert	Refinement FPT_TDC.1.2/NK.TLS.Zert(1)	ST	[gemSpec_PKI]
TIP1-A_4510-05	(Kein SFR)	Abdeckung identisch zu TIP1-A_4510 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4518-02	FDP_ACF.1/AK.TLS	Assignments an FDP_ACF.1.2/AK.TLS(12), (13)	ST	[gemSpec_Kon]
TIP1-A_4524-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4524 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4527-04	(Kein SFR)	Abdeckung identisch zu TIP1-A_4527 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4545-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4545 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4548-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4548 aus PTV2	PP	[gemSpec_Kon]

Afo	SFR		Mapping	Spezifikation
TIP1-A_4561-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4561 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4569-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4569 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4617-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4617 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4623-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4623 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4646-06	(Kein SFR)	Abdeckung identisch zu TIP1-A_4646 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4647-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4647 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4652-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4652 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4653-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4653 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4654-05	(Kein SFR)	Abdeckung identisch zu TIP1-A_4654 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4655-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4655 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4672-05	(Kein SFR)	Abdeckung identisch zu TIP1-A_4672 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4680-03	FDP_ACF.1/AK.TLS FMT_MSA.3/AK.Sig	Durchsetzen der Konfigurationswerte für Komfortsignatur Durchsetzen der Konfigurationswerte für Komfortsignatur	ST	[gemSpec_Kon]
TIP1-A_4696-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4696 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4710-02	FAU_GEN.1/AK	Vgl. ST-Anwendungshinweis 62	ST	[gemSpec_Kon]
TIP1-A_4736-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4736 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4785-03	(Kein SFR)	Abdeckung identisch zu TIP1-A_4785 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4832-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_4832 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4839-01	(Kein SFR)	Abdeckung identisch zu TIP1-A_4839 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_4840-01	(Kein SFR)	Abdeckung identisch zu TIP1-A_4840 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_5437-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_5337 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_5482-01	FPT_TDC.1/AK	Vgl. ST-Anwendungshinweis 59	ST	[gemSpec_Kon]

Afo	SFR		Mapping	Spezifikation
TIP1-A_5484	FDP_ACF.1/AK.SDS	Vgl. ST-Anwendungshinweis 48	ST	[gemSpec_Kon]
TIP1-A_5505	FDP_DAU.2/AK.QES FDP_DAU.2/AK.Sig	Vgl. Ausführungen zu SF.SignatureService Vgl. Ausführungen zu SF.SignatureService	ST	[gemSpec_Kon]
TIP1-A_5538	FDP_ITC.2/AK.Sig FPT_TDC.1.2/AK	Vgl. Ausführungen zu SF.SignatureService Vgl. Ausführungen zu SF.SignatureService	ST	[gemSpec_Kon]
TIP1-A_5540-01	(Kein SFR)	Abdeckung identisch zu TIP1-A_5540 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_5541-01	(Kein SFR)	Abdeckung identisch zu TIP1-A_5541 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_5657-02	(Kein SFR)	Abdeckung identisch zu TIP1-A_5657 aus PTV2	PP	[gemSpec_Kon]
TIP1-A_6025	FDP_ACF.1/AK.Update FPT_FLS.1/AK	Vgl. ST-Anwendungshinweis 39 Vgl. ST-Anwendungshinweis 39	ST	[gemSpec_Kon]
TIP1-A_7254	FTP_ITC.1/AK.FD FTP_ITC.1/AK.VZD	Vgl. Refinement in FTP_ITC.1/AK.FD Vgl. Refinement in FTP_ITC.1/AK.FD	ST	[gemSpec_Kon]
TIP1-A_7255	FMT_MTD.1/AK.Admin	Vgl. ST-Anwendungshinweis 57	ST	[gemSpec_Kon]

Tabelle D.1.: Erweiterung des Security Targets für PTV 5+

Literatur

Schutzprofile und Technische Richtlinien

[AIS 20] Bundesamt für Sicherheit in der Informationstechnik. *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*. Technical Guideline. Version 3. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Mai 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html.

[AIS 31] Bundesamt für Sicherheit in der Informationstechnik. *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*. Technical Guideline. Version 3. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Mai 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.html.

[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-02102-1] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Technische Richtlinie BSI TR-02102-1. Technical Guideline. Version 2018-02. Bundesamt für Sicherheit in der Informationstechnik (BSI), 29. Mai 2018. 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-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-03110-3] Bundesamt für Sicherheit in der Informationstechnik. *Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 3: Common Specifications*. Technische Richtlinie BSI TR-03110-3. Technical Guideline. Version 2.21. Bundesamt für Sicherheit in der Informationstechnik (BSI), 21. Dez. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-3-V2_2.pdf.

[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-03154] Bundesamt für Sicherheit in der Informationstechnik. *Konnektor – Prüfspezifikation für das Fachmodul NFDM*. Technische Richtlinie BSI TR-03154. Technical Guideline. Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Apr. 2019.

[TR-03155] Bundesamt für Sicherheit in der Informationstechnik. *Konnektor – Prüfspezifikation für das Fachmodul AMTS*. Technische Richtlinie BSI TR-03155. Technical Guideline. Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Apr. 2019.

[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.

Spezifikationen

[CAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). CAdES Baseline Profile*. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103173v020101p.pdf.

[CAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). CMS Advanced Electronic Signatures (CAdES)*. ETSI Technical Specification. Version 2.2.1. ETSI, Apr. 2013. URL: http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf.

[PAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). PAdES Baseline Profile*. ETSI Technical Specification. Version 2.2.2. ETSI, Apr. 2013. URL: http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

[PAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). PDF Advanced Electronic Signature Profiles*. Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles. ETSI Technical Specification. Version 1.2.1. ETSI, Juli 2010. URL: http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf.

[SAML2.0] Scott Cantor u. a., Hrsg. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)*. OASIS Open. 15. März 2015. URL: http://docs.oasis-open.org/security/saml/v2.0/.

[TIFF] Adobe Developers Association, Hrsg. *TIFF. Revision 6.0*. Version 6.0. 3. Juni 1992. URL: https://www.adobe.io/open/standards/TIFF.html.

[XAdES-BL] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). XAdES Baseline Profile*. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012. URL: http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.

[XAdES] European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI). XML Advanced Electronic Signatures (XAdES)*. ETSI Technical Specification. Version 1.4.2. ETSI, Dez. 2010. URL: http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf.

[XML] Tim Bray u. a. *Extensible Markup Language (XML)*. W3C Recommendation. W3C, Nov. 2008. URL: http://www.w3.org/TR/xml.

[XMLEnc] Frederick Hirsch u. a. *XML Encryption Syntax and Processing Version 1.1*. W3C Recommendation. W3C, Apr. 2013. URL: http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/.

[XMLSig2] Frederick Hirsch u. a. *XML Signature Syntax and Processing (Second Edition)*. W3C Recommendation. W3C, Juni 2008. URL: http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

[XSLT] Michael Kay. *XSL Transformations (XSLT)*. W3C Recommendation. Version 2.0. W3C, Jan. 2007. URL: http://www.w3.org/TR/2007/REC-xslt20-20070123/.

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_PTV2] gematik GmbH. *Produkttypsteckbrief Konnektor*. Prüfvorschrift. Produkttyp Version PTV2 2.12.0-0. Version 1.0.0. 14. Mai 2018.

[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.

[gemRL_QES_NFDM] gematik GmbH. *Signaturrichtlinie QES. Notfalldaten-Management (NFDM)*. Version 1.4.1. Revision 198508. 2. März 2020.

[gemSpec_COS] gematik GmbH. *Spezifikation des Card Operating System (COS)*. Version 3.14.0. Revision 463868. 16. Mai 2022.

[gemSpec_FM_AMTS] gematik GmbH. *Spezifikation Fachmodul AMTS*. Version 1.4.0. Revision 109470. 15. Mai 2019.

[gemSpec_FM_ePA] gematik GmbH. *Spezifikation Fachmodul ePA*. Version 1.52.0. Revision 531872. 1. Dez. 2022.

[gemSpec_FM_NFDM] gematik GmbH. *Spezifikation Fachmodul NFDM*. Version 1.6.2. Revision 383236. 30. Juni 2021.

[gemSpec_HBA_ObjSys] gematik GmbH. *Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem*. Version 3.13.0. Revision 109544. 15. Mai 2019.

[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.

[gemSpec_SGD_ePA] gematik GmbH. *Spezifikation Schlüsselgenerierungsdienst ePA*. Version 1.5.0. Revision 434675. 31. Jan. 2022.

[gemSpec_SMC-B_ObjSys] gematik GmbH. *Spezifikation der Security Module Card SMC-B Objektsystem*. Version 3.13.0. Revision 109255. 15. Mai 2019.

[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.

[ISO 19005-1] ISO. *Document management – Electronic document file format for long-term preservation. Part 1: Use of PDF 1.4 (PDF/A-1)*. International Standard. International Organization for Standardization, 28. Sep. 2005.

[ISO 19005] ISO. *Document management – Electronic document file format for long-term preservation*. International Standard. International Organization for Standardization, 2005.

[ISO 8859-15] ISO. *Information technology – 8-bit single-byte coded graphic character sets. Part 15: Latin alphabet No. 9*. International Standard. International Organization for Standardization, 12. Feb. 2004.

[NIST SP 800-133] Elaine Barker, Allen Roginsky und Richard Davis. *Recommendation for Cryptographic Key Generation*. NIST Special Publication 800-133. Version 2. National Institute of Standards und Technology, Juni 2020. URL: https://doi.org/10.6028/NIST.SP.800-133r2.

[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 800-38B] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. The CMAC Mode for Authentication*. NIST Special Publication 800-38B. National Institute of Standards und Technology, Mai 2005. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.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 800-56A] Barker u. a. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. NIST Special Publication 800-56A. National Institute of Standards und Technology, Apr. 2018. URL: https://doi.org/10.6028/NIST.SP.800-56Ar3.

[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.

[Unicode] The Unicode Consortium. *The Unicode Standard. Core Specification*. Version 6.2. Hrsg. von Julie D. Allen u. a. Mountain View, CA, 2012. ISBN: 978-1-936213-07-8. URL: http://www.unicode.org/versions/Unicode6.2.0.

RFC

[RFC 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 4122] P. Leach, M. Mealling und R. Salz. *A Universally Unique IDentifier (UUID) URN Namespace*. RFC 4122 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Juli 2005. DOI: 10.17487/RFC4122. URL: https://www.rfc-editor.org/rfc/rfc4122.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 5652] R. Housley. *Cryptographic Message Syntax (CMS)*. RFC 5652 (Internet Standard). RFC. Fremont, CA, USA: RFC Editor, Sep. 2009. DOI: 10.17487/RFC5652. URL: https://www.rfc-editor.org/rfc/rfc5652.txt.

[RFC 5746] E. Rescorla u. a. *Transport Layer Security (TLS) Renegotiation Indication Extension*. RFC 5746 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Feb. 2010. DOI: 10.17487/RFC5746. URL: https://www.rfc-editor.org/rfc/rfc5746.txt.

[RFC 5869] H. Krawczyk und P. Eronen. *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. RFC 5869 (Informational). RFC. Fremont, CA, USA: RFC Editor, Mai 2010. DOI: 10.17487/RFC5869. URL: https://www.rfc-editor.org/rfc/rfc5869.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.

[RUB-XML] Meiko Jensen u. a. „On the Effectiveness of XML Schema Validation-for Countering XML Signature Wrapping Attacks“. In: *XML Schema Validation* 7.1 (1. Jan. 2013). URL: https://www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2013/03/25/paper.pdf (besucht am 18. 12. 2019).

[SEC1-2009] Daniel Brown, Hrsg. *SEC1: Elliptic Curve Cryptography*. Standards for Efficient Cryptography. Version 2.0. Certicom Corp, 21. Mai 2009. URL: https://www.secg.org/sec1-v2.pdf.

[SOG-IS 2020] SOG-IS Crypto WG, Hrsg. *SOGIS Agreed Cryptographic Mechanisms*. Version 1.2. Jan. 2020. URL: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf (besucht am 04. 01. 2023).

[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

1 FDP_IFF.1.2/NK.PF . . . 58
2 FDP_IFF.1.5/NK.PF . . . 59
3 FDP_IFF.1.5/NK.PF(5) . . . 60
4 FPT_STM.1/NK . . . 61
5 FPT_STM.1/NK . . . 61
6 FPT_TDC.1/NK.Zert . . . 61
7 FPT_TDC.1.2/NK.Zert . . . 62
8 FPT_TDC.1.2/NK.Zert . . . 62
9 FPT_TST.1/NK . . . 62
10 FAU_GEN.1.2/NK.SecLog . . . 64
11 FTP_TRP.1.1/NK.Admin . . . 66
12 FMT_MSA.1/NK.PF . . . 67
13 FCS_COP.1.1/NK.Auth . . . 68
14 FCS_CKM.2.1/NK.IKE . . . 69
15 FCS_COP.1.1/NK.TLS.Auth . . . 73
16 FCS_CKM.1.1/NK.Zert . . . 74
17 FMT_MOF.1.1/NK.TLS(3) . . . 77
18 FMT_MOF.1/NK.TLS . . . 77
19 FMT_MOF.1/NK.TLS . . . 77
20 FCS_RNG.1/Hash_DRBG . . . 78
21 FCS_COP.1/AK.AES . . . 85
22 FCS_COP.1/AK.ECIES . . . 86
23 FIA_SOS.1/AK.Passwörter . . . 88
24 FIA_SOS.1/AK.CS.Passwörter . . . 88
25 FIA_UAU.5.1/AK(2) . . . 90
26 FIA_UAU.5.1/AK(5) . . . 90
27 FIA_UAU.5.1/AK(6) . . . 91
28 FIA_API.1/AK.TLS . . . 92
29 FMT_MSA.3/AK.Infomod . . . 93
30 FDP_ACF.1.4/AK.eHKT . . . 96
31 FDP_ACF.1.2/AK.KD(1) . . . 101
32 FDP_DAU.2.1/AK.QES . . . 112
33 FDP_DAU.2.1/AK.QES . . . 112
34 FDP_DAU.2.1/AK.Sig . . . 114
35 FMT_MSA.1/AK.User . . . 117
36 FTP_ITC.1.3/AK.QSEE . . . 118
37 FTA_TAB.1/AK.SP . . . 118
38 FDP_ACF.1.4/AK.Update . . . 121
39 FDP_ACF.1.1/AK.Update (für TIP1-A_6025) . . . 121

40 FDP_ACF.1/AK.Enc . . . 125
41 FDP_ITC.2.5/AK.Enc(2) . . . 125
42 FDP_ETC.2.4/AK.Enc(2) . . . 126
43 FDP_ACC.1/AK.TLS . . . 127
44 FDP_ACF.1.2/AK.TLS . . . 130
45 FMT_MSA.1/AK.TLS . . . 130
46 FMT_MSA.3.2/AK.TLS . . . 131
47 FTP_ITC.1/AK.FD . . . 131
48 FDP_ACF.1.1/AK.SDS(3) (für TIP1-A_5484) . . . 136
49 FDP_ACF.1.4/AK.SDS(1) . . . 137
50 FMT_MSA.1/AK.VSDM . . . 139
51 FMT_MSA.3/AK.VSDM . . . 139
52 FMT_MSA.4.1/AK . . . 141
53 FMT_MOF.1.1/AK . . . 144
54 FMT_MTD.1.1/AK.Admin(5), (6) . . . 145
55 FMT_MTD.1.1/AK.Admin(7) . . . 145
56 FMT_MTD.1.1/AK.Admin(12) . . . 146
57 FMT_MTD.1.1/AK.Admin(16) (für TIP1-A_7255) . . . 146
58 FMT_MTD.1/AK.Zert . . . 146
59 FPT_TDC.1.1/AK (für TIP1-A_5482-01) . . . 147
60 FPT_TDC.1.1/AK(6) . . . 147
61 FPT_TST.1.3/AK.Run-time . . . 150
62 FAU_GEN.1/AK (für TIP1-A_4710-02), (für VSDM-A_2789) . . . 152
63 FAU_STG.4.1/AK . . . 153
64 FTP_ITC.1/VAU . . . 154
65 FTP_ITC.1/VAU . . . 154
66 FCS_COP.1/VAU.Hash . . . 155
67 FCS_CKM.1.1/VAU . . . 155
68 FCS_COP.1/VAU.ECDSA . . . 156
69 FPT_TDC.1/VAU.Zert . . . 157
70 FTP_ITC.1/VAU . . . 158
71 FDP_ACF.1/SGD . . . 161
72 FCS_COP.1/SGD.ECDSA . . . 162
73 FCS_COP.1/SGD.ECIES . . . 164
74 FCS_COP.1/SGD.ECIES . . . 164

Index der gematik Anforderungen

A_14223 . . . . . 219, **235**
A_14930 . . . . . 219, **235**
A_15210 . . . . 205, 206, 219, **235**
A_15532 . . . . . 219, **235**
A_15549 . . . . . 204, 206, **235**
A_15561 . . . . . **235**
A_15590 182
A_16203 . . . . . **235**
A_16849 . . . . . 204, **235**
A_16852-01 . . . . . 155, 206, **235**
A_16883-01 . . . . . 205, **235**
A_16884 . . . . . 204, **235**
A_16897 . . . . . 205, **235**
A_16899 . . . . . **235**
A_16900 . . . . . 204, **235**
A_16903 . . . . . 205, 206, **235**
A_16941-01 156, 157, 205, 206, **235**
A_16943-01 . 155, 206, 207, **235**
A_16945-02 . 157, 205, 207, **236**
A_16957-01 . . . . . 205, **236**
A_16958 . . . . . 205, **236**
A_17069 . . . . . 205, **236**
A_17070-02 . 157, 205, 206, **236**
A_17071 . . . . . 205, 206, **236**
A_17074 . . . . . 204, **236**
A_17081 . . . . . 205, 206, **236**
A_17084 . . . . 157, 205, 207, **236**
A_17094-01 . . . . . 72, 73, **236**
A_17124-01 . . . . . 72, 73, **236**
A_17125 . . . . . 68, **236**
A_17205 181
A_17205 . . . . . **236**
A_17206 . . . . . **237**
A_17207 . . . . . **237**
A_17208 . . . . . **237**
A_17209 . . . . . **237**
A_17210 . . . . . **237**
A_17220 . . . . . 85, 87, 197, **237**
A_17221-01 . . . . . **237**
A_17225-01 . . . . . 205, 206, **237**
A_17322 . . . . . **237**
A_17345 61
A_17359 . . . . . **237**
A_17360 . . . . . **237**
A_17548-01 . . . . . **237**
A_17549-01 . . . . . **238**
A_17661 . . . . . **238**
A_17688 . . . . . **238**
A_17690 . . . . . **238**
A_17746 . . . . . **238**
A_17768 . . . . . **238**
A_17777 . . . . . **238**
A_17821 . . . . . 61, **238**
A_17837-01 . . . . . 61, **238**
A_17847 . . . . . **238**
A_17848 . . . . . **238**
A_17872 . . . . . 163, 238
A_17874 . . . . 163, 209, 238, **239**
A_17875 163
A_17875 163, 209, 210, 238, **239**
A_17888 . . . . . 210, **239**
A_17889 . . . . . 208, **239**
A_17892 . . . . . 208, **239**
A_17893 . . . . . 208, **239**
A_17894-01 . . . . . 208, **239**
A_17895-01 . . . . . 208, **239**
A_17897 . . . . . 159, 208, **239**
A_17898 . . . . . 210, **239**
A_17899 . . . . . 208, **239**
A_17900 . . . . . 209, **239**
A_17901 . . . . . 209, **239**
A_17902 . . . . . 209, 210, **239**
A_17903 . . . . . 209, 210, **240**
A_17924-01 . . . . . 210, **240**
A_17930 . . . . . **240**
A_18001 . . . . . **240**
A_18002 . . . . . **240**
A_18003 . . . . . 210, **240**
A_18004 . . . . . **240**
A_18005 . . . . . 209, **240**
A_18006 . . . . . 210, **240**
A_18021 . . . . . 209, **240**
A_18024 . . . . 160–162, 208, **240**
A_18025-01 . . . . . 209, **240**
A_18028 . . . . . 209, **240**
A_18029 . . . . . 210, **240**
A_18031-01 . . . . . 210, **240**
A_18032 . . . . . **241**
A_18390 . . . . . 121, 145, 200
A_18391 . . . . . 121, 145, 201
A_18464 . . . . . 77, **241**
A_18465-01 . . . . . 205, **241**
A_18466-01 . . . . . 204, **241**
A_18467 . . . . . **241**
A_18597 141
A_18624 . . . . . **241**
A_18686-01 116
A_18686-01 . . . . . 108, 196, **241**
A_18756 . . . . . **241**
A_18987 . . . . . 208, **241**
A_18988 . . . . . 208, **241**
A_19000 . . . . . 208, **241**
A_19052-01 . . . . . **241**
A_19100-01 . . . . . 108, 196, **241**
A_19101 . . . . . 46, 196, **241**
A_19102-04 . . . . . **241**
A_19103-07 . . . . . **241**
A_19104-04 . . . . . 116, **241**
A_19105 197
A_19105 . . . . . 108, 197
A_19106-02 116
A_19108 108
A_19258 . . . . . 118, 196, **241**
A_19738 . . . . . **241**
A_19971 . . . . . 208, 209, **242**
A_20073-01 . . . . . 90, 196, **242**

A_20074 . . . . . 90, 196, **242**
A_20469-02 61
A_20478 . . . . . 194, 241, **242**
A_20549 . . . . . 204, **242**
A_20977 . . . . . 210, **242**
A_21185 . . . . . 61, 62, **242**
A_21275-01 . . . . . 73, **242**
A_21697-01 . . . . . 75, **242**
A_21698 . . . . . 76, **242**
A_21699-02 . . . . . 74, 172, **242**
A_21701 . . . . . 75, **242**
A_21702 . . . . . 76, **242**
A_21749-03 . . 75, 119–121, 148, 149, **242**
A_21759 121
A_21760-01 . . . . . 76, **242**
A_21811-03 . . . . . **242**
A_21879 . . . . . 75, **242**
A_21888 . . . . . 205, **242**
A_22344 . . . . . 196, **243**
A_22352 . . . . . 196, **243**
A_22458 . . . . . 90, **243**
A_22459 . . . . . 196, **243**
A_22494 . . . . . **243**
A_22497 . . . . . **243**
A_22673 . . . . . 194, **243**
A_22923 . . . . . 194, **243**
A_23226-01 . . . . . **243**

GS-A_4357-02 73, 156, 161, 182, 183
GS-A_4358-01 . . . . . 182, 183
GS-A_4376-02 . . . . . 197, **243**
GS-A_4384-01 . . . . . 72, 92, 172
GS-A_4390 197
GS-A_4446-05 . 71, 157, 219, **243**
GS-A_4651 . . . . . **243**
GS-A_4652-01 157
GS-A_4663 71
GS-A_4663 . . . . . **243**
GS-A_4898 61
GS-A_5016 . . . . 85–87, 157, 163
GS-A_5131 . . . . . 155, 157
GS-A_5215 . . . . . 71, 148
GS-A_5345-01 72

TIP1-A_4510-05 . . . . . 235, **243**
TIP1-A_4516 90
TIP1-A_4517-02 73
TIP1-A_4518-02 . . . . . **243**
TIP1-A_4524-03 . . 196, 197, **243**
TIP1-A_4527-04 . . . . . **243**
TIP1-A_4545-03 . . . . . **243**
TIP1-A_4548-02 . . . . . **243**
TIP1-A_4558 101
TIP1-A_4560 108
TIP1-A_4561-02 . . . . . **244**
TIP1-A_4569-02 . . . . . **244**
TIP1-A_4617-02 . . . . . 197, **244**
TIP1-A_4623-02 . . . . . **244**
TIP1-A_4646-06 . . . . . **244**
TIP1-A_4647-03 . . . . . **244**
TIP1-A_4652-02 . . . . . **244**
TIP1-A_4653-03 . . . . . **244**
TIP1-A_4654-05 . . . . . **244**
TIP1-A_4655-03 . . . . . **244**
TIP1-A_4670 118
TIP1-A_4671 108
TIP1-A_4672-05 . . . . . **244**
TIP1-A_4680-03 . . 195, 196, **244**
TIP1-A_4696-02 . . . . . **244**
TIP1-A_4710-02 . . . . . 152, **244**
TIP1-A_4736-02 . . . . 54, 55, **244**
TIP1-A_4747 59
TIP1-A_4785-03 . . . . . **244**
TIP1-A_4808-01 88
TIP1-A_4832-02 . . . . . **244**
TIP1-A_4835-02 201
TIP1-A_4839-01 . . . . . **244**
TIP1-A_4840-01 . . . . . **244**
TIP1-A_4843 60
TIP1-A_5009 130
TIP1-A_5437-02 . . . . . **244**
TIP1-A_5439 195
TIP1-A_5482-01 . . . . . 147, **244**
TIP1-A_5484 . . . . . 136, **245**
TIP1-A_5505 . . . . . **245**
TIP1-A_5538 . . . . . 193, **245**
TIP1-A_5540-01 . . . . . **245**
TIP1-A_5541-01 . . . . . **245**
TIP1-A_5657-02 . . . . . **245**
TIP1-A_6025 . . . . . 121, **245**
TIP1-A_6031 101
TIP1-A_6478 96
TIP1-A_7254 . . . . . 131, **245**
TIP1-A_7255 . . . . . 146, **245**

VSDM-A_2789 152

Index der SFR

FAU_GEN.1/AK **151**, 196, 204, 218, 244
FAU_GEN.1/NK.SecLog **63**, 152, 179, 221
FAU_GEN.2/NK.SecLog **64**, 179
FAU_SAR.1/AK **152**, 204
FAU_STG.1/AK **153**, 203
FAU_STG.4/AK **153**, 203, 218
FCS_CKM.1/AK.AES **80**, 85, 185, 198
FCS_CKM.1/NK **69**, 184
FCS_CKM.1/NK.Auth **74**, 76, 167, 172, 185, 242
FCS_CKM.1/NK.TLS **71**, 181, 184, 218, 236, 243
FCS_CKM.1/NK.Zert **73**, 172, 185, 218, 236, 242
FCS_CKM.1/VAU **155**, 168, 171, 205, 206, 222, 235
FCS_CKM.2/NK.IKE **69**, 184
FCS_CKM.4/AK . . **81**, 84, 168, 169, 171, 172, 185, 209, 235, 240
FCS_CKM.4/NK **69**, 74, 167, 177, 184
FCS_COP.1/AK.AES **85**, 198, 221, 240
FCS_COP.1/AK.CMS.Ent **87**, 197, 221, 237, 238
FCS_COP.1/AK.CMS.Sign **82**, 191, 221, 237, 238
FCS_COP.1/AK.CMS.SigPr **83**, 191, 237, 238
FCS_COP.1/AK.CMS.Ver **87**, 197, 221, 237, 238
FCS_COP.1/AK.ECIES **85**, 169, 173, 198, 237
FCS_COP.1/AK.PDF.Sign **82**, 191, 221, 237, 238
FCS_COP.1/AK.PDF.SigPr **83**, 191, 237, 238
FCS_COP.1/AK.SHA **80**, 82–84, 185
FCS_COP.1/AK.SigVer.BNetzA-VL **84**, 168, 172, 186
FCS_COP.1/AK.SigVer.ECDSA . . **81**, 83, 84, 191, 236, 237
FCS_COP.1/AK.SigVer.PSS **81**, 83, 84, 191
FCS_COP.1/AK.SigVer.SSA **81**, 83, 84, 191
FCS_COP.1/AK.XML.Ent **86**, 197, 221
FCS_COP.1/AK.XML.Sign . . . **81**, 191, 221, 237, 238, 242
FCS_COP.1/AK.XML.SigPr **82**, 191, 221, 237, 238
FCS_COP.1/AK.XML.Ver **86**, 197, 221
FCS_COP.1/NK.Auth **67**, 182, 184, 236
FCS_COP.1/NK.ESP **68**, 184
FCS_COP.1/NK.Hash **67**, 181
FCS_COP.1/NK.HMAC **67**, 181, 184
FCS_COP.1/NK.IPsec **68**, 184
FCS_COP.1/NK.SigVer **78**, 137, 167, 172, 182, 236
FCS_COP.1/NK.TLS.AES **72**, 181, 184, 218
FCS_COP.1/NK.TLS.Auth **73**, 74, 156, 162, 167, 184, 218, 242
FCS_COP.1/NK.TLS.HMAC **72**, 181, 184, 218
FCS_COP.1/SGD.ECDSA . . . **161**, 169, 171, 208–210, 222, 238–240
FCS_COP.1/SGD.ECIES . . . **162**, 169, 171, 209, 210, 222, 238–241
FCS_COP.1/SGD.Hash **158**, 168, 172, 208, 209, 222, 238, 239, 242
FCS_COP.1/Storage.AES **80**, 137, 167, 172, 184
FCS_COP.1/VAU.AES **157**, 168, 171, 206, 207, 222, 235, 236, 240
FCS_COP.1/VAU.ECDSA **155**, 168, 171, 206, 222
FCS_COP.1/VAU.Hash **154**, 168, 171, 205, 206, 222, 235, 236
FCS_RNG.1/Hash_DRBG 73, 74, **77**, 81, 85–87, 155, 157, 163, 167, 171, 172, 181, 184, 185, 206, 207, 209, 210
FDP_ACC.1/AK.eHKT **93**, 189, 190, 220
FDP_ACC.1/AK.Enc **122**, 197
FDP_ACC.1/AK.Infomod **92**, 188, 189, 220
FDP_ACC.1/AK.KD **98**, 191, 220, 221
FDP_ACC.1/AK.PIN **101**, 191, 220
FDP_ACC.1/AK.SDS **134**, 199, 222
FDP_ACC.1/AK.Sgen **105**, 192
FDP_ACC.1/AK.SigPr **109**, 192, 221
FDP_ACC.1/AK.TLS **126**, 168, 186, 221
FDP_ACC.1/AK.Update **119**, 201, 242
FDP_ACC.1/AK.VSDM 60, **137**, 199
FDP_ACC.1/SGD **159**, 168, 171, 208, 222, 239, 240
FDP_ACF.1/AK.eHKT **94**, 189, 190, 220
FDP_ACF.1/AK.Enc 89, **122**, 197
FDP_ACF.1/AK.Infomod **92**, 188, 189, 197, 220
FDP_ACF.1/AK.KD **98**, 191, 220, 221
FDP_ACF.1/AK.PIN **102**, 191, 220
FDP_ACF.1/AK.SDS **135**, 199, 222, 245
FDP_ACF.1/AK.Sgen . **106**, 169, 192, 195–197, 221, 241
FDP_ACF.1/AK.SigPr 89, **110**, 192, 221

FDP_ACF.1/AK.TLS **127**, 186, 196, 221, 243, 244
FDP_ACF.1/AK.Update **119**, 143, 201, 242, 245
FDP_ACF.1/AK.VSDM 60, **137**, 199
FDP_ACF.1/SGD **160**, 168, 171, 208, 222, 239, 240
FDP_DAU.2/AK.Cert **114**, 193
FDP_DAU.2/AK.QES **111**, 193, 194, 218, 221, 245
FDP_DAU.2/AK.Sig **113**, 193, 194, 245
FDP_ETC.2/AK.Enc **125**, 197, 221, 240
FDP_ETC.2/NK.TLS **75**, 185, 218, 242
FDP_IFC.1/NK.PF **54**, 66, 175
FDP_IFF.1/NK.PF **54**, 66, 175, 177
FDP_ITC.2/AK.BNetzA-VL 84, **134**, 168, 172, 186
FDP_ITC.2/AK.Enc 86, **125**, 169, 197, 221, 240
FDP_ITC.2/AK.Sig **115**, 192, 220, 245
FDP_ITC.2/NK.TLS **74**, 76, 185, 218, 242
FDP_ITC.2/SGD **159**, 168, 169, 171, 208, 222, 239, 240
FDP_RIP.1/AK **141**, 203, 235
FDP_RIP.1/NK **62**, 177
FDP_SDI.2/AK **116**, 192, 193
FDP_UCT.1/AK.TLS **96**, 186, 189, 190
FDP_UIT.1/AK.TLS **96**, 186, 189, 190
FDP_UIT.1/AK.Update **121**, 201
FIA_API.1/AK **91**, 187, 188
FIA_API.1/AK.TLS **91**, 168, 172, 186
FIA_SOS.1/AK.CS.Passwörter **88**, 168, 173, 187, 188
FIA_SOS.1/AK.Passwörter **87**, 173, 187, 188
FIA_SOS.2/AK.Jobnummer **105**, 192
FIA_SOS.2/AK.PairG **88**, 187, 188
FIA_UAU.1/AK **89**, 188
FIA_UAU.5/AK **89**, 129, 187, 188, 192, 196, 220, 241–243
FIA_UID.1/AK **89**, 188
FIA_UID.1/NK.SMR **65**, 180, 200
FMT_MOF.1/AK **143**, 200
FMT_MOF.1/NK.TLS 66, **75**, 91, 184, 218, 241, 242
FMT_MSA.1/AK.Infomod **93**, 189
FMT_MSA.1/AK.TLS **130**, 187, 188, 200
FMT_MSA.1/AK.User **117**, 193, 194, 220
FMT_MSA.1/AK.VSDM **139**, 199
FMT_MSA.1/NK.PF **66**, 176, 180
FMT_MSA.3/AK.Infomod **93**, 189
FMT_MSA.3/AK.Sig **116**, 143, 145, 192, 196, 244
FMT_MSA.3/AK.TLS **130**, 143, 187, 188, 200
FMT_MSA.3/AK.VSDM **139**, 199
FMT_MSA.3/NK.PF **60**, 66, 175
FMT_MSA.4/AK **139**, 169, 191, 192, 221
FMT_MSA.4/NK **67**, 180
FMT_MTD.1/AK.Admin 143, **144**, 200, 241, 245
FMT_MTD.1/AK.eHKT_Abf **96**, 143, 189, 190
FMT_MTD.1/AK.eHKT_Mod **97**, 143, 189, 190
FMT_MTD.1/AK.Zert 143, **146**, 191, 220
FMT_MTD.1/NK **65**, 180
FMT_SMF.1/AK **142**, 200
FMT_SMF.1/NK **66**, 180
FMT_SMR.1/AK **142**, 200
FMT_SMR.1/NK **64**, 180
FPT_EMS.1/NK **62**, 179
FPT_FLS.1/AK **149**, 152, 203, 235, 245
FPT_STM.1/AK **151**, 204, 222
FPT_STM.1/NK **60**, 64, 143, 177, 222
FPT_TDC.1/AK 143, **147**, 168, 172, 186, 221, 238, 244, 245
FPT_TDC.1/NK.TLS.Zert **70**, 184, 218, 219, 221, 235, 243
FPT_TDC.1/NK.Zert **61**, 175, 221, 238, 242
FPT_TDC.1/SGD.Zert **162**, 169, 171, 208, 221, 222, 238, 240
FPT_TDC.1/VAU.Zert **156**, 168, 171, 206, 219, 221, 222, 235–237, 243
FPT_TEE.1/AK **149**, 189–191, 218, 220
FPT_TST.1/AK.Out-Of-Band **150**, 203
FPT_TST.1/AK.Run-time **150**, 203, 237
FPT_TST.1/NK **62**, 178, 203
FTA_TAB.1/AK.Jobnummer **118**, 192
FTA_TAB.1/AK.SP **118**, 192
FTP_ITC.1/AK.CS **132**, 186
FTP_ITC.1/AK.eHKT **133**, 186, 189, 190
FTP_ITC.1/AK.FD **131**, 138, 143, 186, 245
FTP_ITC.1/AK.KSR **132**, 186
FTP_ITC.1/AK.QSEE **117**, 188, 192, 196, 241
FTP_ITC.1/AK.TSL **132**, 168, 186, 238
FTP_ITC.1/AK.VZD **131**, 186, 245
FTP_ITC.1/NK.TLS **70**, 76, 218, 236, 237
FTP_ITC.1/NK.VPN_SIS **53**, 174
FTP_ITC.1/NK.VPN_TI **53**, 174
FTP_ITC.1/SGD **158**, 168, 171, 208–210, 222, 239–242
FTP_ITC.1/VAU **153**, 168, 171, 204–207, 222, 235, 236, 241, 242
FTP_TRP.1/NK.Admin 54, 55, **65**, 180, 200