Common Criteria Certification
BSI-DSZ-CC-1159

Security Target

ePA Modul Frontend des Versicherten
Version v1.0.7

cgm AG
Maria Trost 21
56070 Koblenz

Dokumentversion 1.29
2021-07-18

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einführung in das Security Target

Der Evaluierungsgegenstand (Target of Evaluation - TOE), der in diesem Dokument beschrieben wird, ist das *ePA Modul FdV* in der Version *v1.0.7*. Der TOE ist eine sichere Software, die als ePA Modul FdV ergänzt um eine Komponente zur al.vi-Authentifzierung gegenüber dem Signaturdienst im Rahmen der elektronischen Patientenakte (ePA) eingesetzt wird.

Das Modul ist eine Komponente des ePA Frontend des Versicherten und ein Teil der ePA-Plattform. Die weiteren Komponenten des ePA Frontend des Versicherten sowie die ePA-Plattform insgesamt sind nicht Teil dieses TOEs.

Dieses Dokument ist das *Security Target*, in dem die funktionalen und organisatorischen Sicherheitsanforderungen des TOEs und seiner Einsatzumgebung beschrieben werden.

Eine Liste der referenzierten Dokumente findet sich im Literaturverzeichnis am Ende des Dokuments.

1.1. ST Referenz

Titel des Dokuments	Security Target / ePA Modul FdV
Version des Dokuments	1.29
Datum des Dokuments	18.07.2021
Allgemeiner Status	
Autor	CompuGroup Medical Deutschland AG
Editor	

Darüber hinaus orientiert sich dieses Dokument in fachlicher Hinsicht an den relevanten Spezifikationen der gematik, die im Anhang aufgeführt sind; allen voran die FdV-Spezifikation [gemSpec_Frontend_Vers], dem Addendum [gemSpec_FrontendVersUEePA] und dem Produktsteckbrief [gemProdTePAModulFdV].

1.2. TOE Referenz

Evaluierungsgegenstand	ePA Modul FdV in der Version v1.0.7
Version des EVG	v1.0.7
Hersteller	CompuGroup Medical Deutschland AG
Vertrauenswürdigkeitsstufe	EAL2 (Kurzbezeichnung „EAL2“)
CC Version	3.1 Release 5

1.3. Überblick über den TOE

Der TOE ist das *ePA Modul FdV* in der Version *v1.0.7*. Das Modul ist Teil der ePA-Infrastruktur zur wechselseitigen Bereitstellung von Dokumenten für Leistungserbringer und gesetzliche Versicherte.

Der Lieferumfang des TOE umfasst ebenfalls die Betriebsdokumentation für das ePA Modul FdV.

1.3.1. TOE Typ

Der TOE implementiert den Produkttyp eines ePA Modul FdV für ein Frontend des Versicherten für die elektronische Patientenakte [gemProdTePAModulFdV]. Der Funktionsumfang ist gemäß dem Addendum [gemSpec_FrontendVersUEePA] eingeschränkt. Der TOE besteht ausschließlich aus Software. Er ist als Softwarepaket bestehend aus kompilierten C++ Bibliotheken und einem Plugin zur Verwendung der Bibliotheken mit Flutter konzipiert, die von einer Anwendung auf einem mobilen Endgerät eingebunden wird. Der TOE kapselt die Funktionalität des Protokollendpunkt des ePA-Gesamtsystem-Sicherheitskonzepts, inklusive aller Kryptographie und Kommunikation mit den Diensten der Telematikinfrastruktur, was auch die lokale Kommunikation mit der eGK und die Authentifizierung gegenüber dem Signaturdienst zur Implementierung der alternativen Versichertenidentität (al.vi) beinhaltet.

Die Verantwortung für den Betrieb und die Integration des ePA Modul FdV liegt beim Entwickler des ePA Frontend des Versicherten.

1.3.2. Verwendung und Hauptfunktionalität des TOE

Das gesamte ePA-Aktensystem eines Anbieters setzt sich aus den logischen Bestandteilen Authentifizierung von Nutzern, Autorisierung und Schlüsselverwaltung, Dokumentenverwaltung und dem Zugangsgateway zusammen.

Der TOE ist ein sicheres Software-Modul für den Versicherten, welches die für den Versicherten notwendigen Funktionalitäten zur Nutzung des ePA-Aktensystems bündelt und dezentrale Fachlogik der Fachanwendung ePA ausführt.

Der TOE ermöglicht insbesondere die sichere Verbindung vom Gerät des Versicherten (GdV) zum Zugangsgateway des Aktensystems und die sichere Anbindung der eGK durch den Einsatz kryptographischer Methoden und der Prüfung der Authentizität der Kommunikationspartner. Für den Anwendungsentwickler stellt der TOE Schnittstellen zur Nutzung der ePA-Fachlogik bereit. Er abstrahiert damit die Komplexität des VAU-Server-Protokolls, welches er intern umsetzt. Er verbirgt die Smartcard-Kommunikation zur eGK über die Schnittstellen des Endgerätes. Der TOE unterstützt anstelle der eGK auch die Nutzung der alternative Versichertenidentität (al.vi) mittels eines Signaturdienstes und gewährleistet in diesem Zusammenhang insbesondere die sichere Ablage des Authentifizierungsmaterials auf dem GdV.

Des Weiteren umfassen seine Hauptfunktionalitäten die Auswahl verschiedener Aktionen (u. a. Dokumente suchen, Dokumente einstellen, Protokolldaten einsehen) sowie das Verschlüsseln und Entschlüsseln von Dokumenten.

Der TOE setzt gemäß den Übergangsregelungen ePA [gemSpec_FrontendVersUEePA] nicht die Funktionen Anbieterwechsel, Vertreterregelungen und Bereitstellung und Verarbeitung Kostenträgerdokumente um.

1.3.3. Erforderliche Non-TOE Hardware/Software/Firmware

Der TOE wird in eine Anwendung integriert, welche dem Versicherten eine grafische Benutzeroberfläche (GUI) bereitstellt und es ihm so ermöglicht, ePA-Anwendungsfälle auszuführen. Die Eigenschaften der GUI sind nicht normativ durch die Spezifikation vorgegeben, die GUI ist nicht Bestandteil des vorliegenden TOEs. Sie ist ein Teil der direkten Umgebung des TOEs.

TOE und GUI gemeinsam bilden das ePA Frontend des Versicherten (FdV). Die in der Spezifikation [gemSpec_Frontend_Vers] zugelassene Option, dass das FdV darüber hinaus zusätzliche Funktionen beinhalten könnte (bspw. kassenspezifische Funktionen, welche Schnittstellen zu kassenspezifischen Diensten außerhalb der TI nutzen) wird aktuell nicht umgesetzt.

Der TOE besitzt eine produktspezifische, anwendungsinterne Schnittstelle, welche durch das GUI oder die zusätzlichen Funktionalitäten der integrierenden Anwendung genutzt werden kann, um ePA-Anwendungsfälle auszuführen.

Ausführungsumgebung des FdV ist ein mobiles Endgerät, das im weiteren als Gerät des Versicherten (GdV) bezeichnet wird. Es steht unter alleiniger Kontrolle des Versicherten. Dem Versicherten obliegt es, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken. Das FdV setzt ein GdV mit einer der folgenden Plattformen voraus:

- Android Geräte mit 64-bit-Architektur ARMv8 und:
  - Android Version 8 oder 8.1
  - Android Version 9
  - Android Version 10
  - Android Version 11
- iOS Geräte mit:
  - iOS Version 13 oder 14

Zur Nutzung der Hauptanwendungsfälle der Anwendung, und damit auch des TOEs, ist entweder eine eGK oder eine alternative Versichertenidentität (al.vi) notwendig. Für die Nutzung der eGK wird auf dem mobilen Endgerät eine NFC-Schnittstelle vorausgesetzt.

1.4. Beschreibung des TOEs

1.4.1. Hauptziele des TOEs

Der TOE ist ein Softwarepaket, das von den Entwicklern des FdV eingebunden wird. Das ePA Modul FdV abstrahiert die Logik zur Kommunikation mit dem ePA-Aktensystem. Das bedeutet, dass der TOE neben TLS, das VAU-Server-Protokoll zur Absicherung der Kommunikation mit der Dokumentenverwaltung und das ECIES-Protokoll zur Absicherung der Kommunikation mit den Schlüsselgenerierungsdiensten umsetzt. Dem Entwickler des FdV steht somit eine technische Abstraktion zur Nutzung aller ePA Funktionalität zur Verfügung, die über eine fest spezifizierte Schnittstelle nutzbar ist. Gleichzeitig wird die Kommunikation mit der eGK über eine Kontaktlos-Schnittstelle gekapselt, so dass der FdV Entwickler von dieser Komplexität abgeschirmt wird. Hierzu nutzt das ePA Modul FdV Funktionen des Betriebssystems, welches die technische Anbindung zur Kommunikation bereitstellt. Die Sicherheitseigenschaften der Kommunikation garantiert der TOE selbst, der die entsprechende

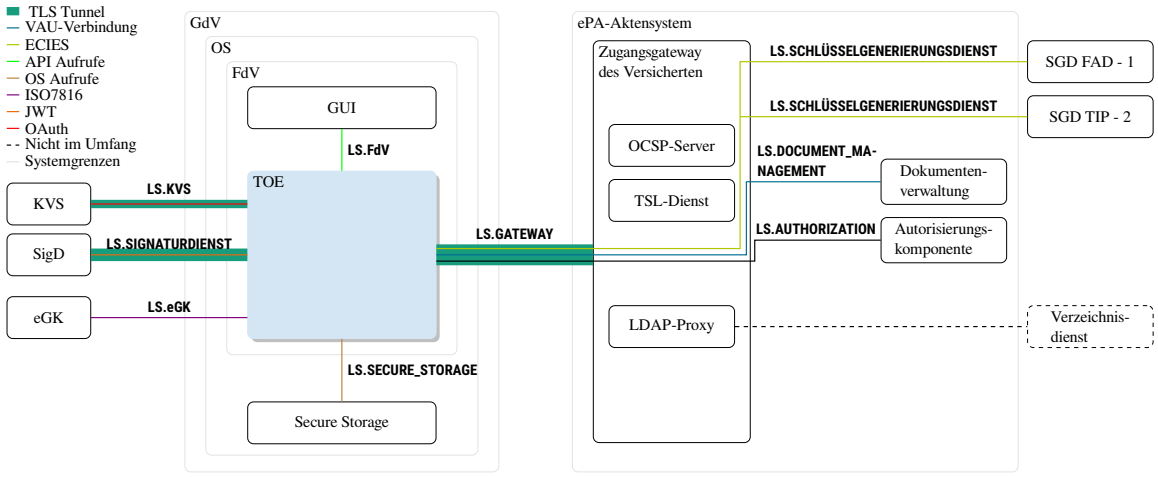

Abbildung 1.1.: Abbildung der Einsatzumgebung des TOEs

Funktionalität umsetzt. Außerdem stellt der TOE eine Schnittstelle bereit für die Nutzung des Signaturdienstes inklusive der Beantragung einer al.vi und der Registrierung des GdV über das Kontoverwaltungssystem (KVS) CGM Life von CGM. Die Schnittstelle abstrahiert dabei die technischen Details der verwendet Protokolle und nutzt Funktionen des Betriebssystems um Authentifizierungsmerkmale gegenüber dem Signaturdienst lokal sicher abzulegen.

1.4.2. Einsatzumgebung des TOEs

Im Folgenden werden die einzelnen Komponenten der Einsatzumgebung des TOEs aufgezählt und erklärt (siehe Abbildung 1.1):

Anwendung Frontend des Versicherten (FdV) ist die gesamte Applikation, die auf dem GdV läuft.

Authorisierungskomponente stellt authentifizierten Nutzern eines Aktenkontos bei gegebener Autorisierung das für sie jeweils empfängerverschlüsselte Schlüsselmaterial bereit. Neben der zentralen Verwaltung des empfängerbezogenen verschlüsselten Schlüsselmaterials erfolgt hierbei auch ein Berechtigungserhalt für Versicherte.

Betriebssystem (OS) bezeichnet das Betriebssystem des GdV, konkret werden Android Version 8, 8.1, 9, 10 und 11 sowie iOS Version 13 und 14 unterstützt.

Dokumentenverwaltung stellt ein Dokumentenmanagementsystem mit der medizinischen Dokumentation des Versicherten dar.

Elektronische Gesundheitskarte (eGK) stellt ein Authentifizierungsverfahren und eine Quelle für Zufall bereit.

Gerät des Versicherten (GdV) ist das mobile Endgerät des Anwenders, also Smartphone oder Tablet. Es stellt die Ausführungsumgebung für das FdV und damit den TOE dar.

Grafische Benutzeroberfläche (GUI) ist die für die Nutzung des TOEs notwendige GUI. Sie ist Teil des FdV.

LDAP-Proxy ist eine Komponente des Zugangsgateways, die für den Zugriffe auf den Verzeichnisdienst der TI-Plattform verwendet wird.

Kontoverwaltungssystem (KVS) ermöglicht es dem TOE, eine al.vi zu beantragen. Das KVS wird durch das System CGM Life realisiert.

OCSP-Server dient zur Prüfung des Online-Status von Zertifikaten der Telematikinfrastruktur. Zugriffe auf den OCSP-Dienst der TI-Plattform erfolgen nur über die Komponente Zugangsgateway.

Schlüsselgenerierungsdienst (SGD) generiert berechtigtenindividuelle symmetrische Schlüssel zur Verschlüsselung und Entschlüsselung von Akten- und Kontextschlüssel. Es gibt insgesamt zwei, mit SGD1 und SGD2 bezeichnete Schlüsselgenerierungsdienste.

Secure Storage ist ein durch das Betriebssystem auf dem Gerät des Versicherten bereitgestellter sicherer Speicher. Konkret verwendet das ePA Frontend des Versicherten die KeyChain von iOS und den KeyStore von Android.

Signaturdienst (SigD) erzeugt alternative elektronische Identifizierungsmittel für Versicherte in der Umgebung des Anbieters des Signaturdienstes.

TSL-Dienst stellt die TSL-Datei bereit und dient auch der Verteilung weiterer kryptographischer Infrastruktur-Elemente. Die TSL-Datei ist eine signierte Whitelist der zugelassenen Zertifikatsherausgeber. Das heißt, die TSL-Datei enthält sämtliche nonQES-X.509-CA-Zertifikate, die in der Telematikinfrastruktur verwendet werden. Des Weiteren enthält sie die nötigen Informationen für die Statusprüfung der von den CAs ausgestellten End-Entity-Zertifikate innerhalb der Telematikinfrastruktur. Dies geschieht in Form der Adressen und Zertifikate der zuständigen OCSP-Responder. Zugriffe auf den TSL-Dienst der TI-Plattform erfolgen nur über die Komponente Zugangsgateway.

Verzeichnisdienst (VZD) ist ein zentraler Dienst der TI-Plattform. Er beinhaltet die Speicherung aller Einträge von Leistungserbringern und Institutionen mit allen definierten Attributen, die in das Verzeichnis aufgenommen werden sollen und die Fachdaten durch fachanwendungsspezifische Dienste.

Zugangsgateway des Versicherten ermöglicht dem TOE die sichere Nutzung des ePA-Aktensystems über das Internet.

1.4.3. Hardware des TOEs

Der TOE beinhaltet keine Hardware.

1.4.4. Schnittstellen des TOEs

Im Folgenden werden die physischen und logischen Schnittstellen des TOEs kurz beschrieben.

1.4.4.1. Physische Schnittstellen

Der TOE hat keine physischen Schnittstellen.

1.4.4.2. Logische Schnittstellen

Der TOE verfügt über die folgenden logischen Schnittstellen.

LS.AUTHORIZATION ist die Schnittstelle des TOE zur Autorisierungskomponente des ePA-Aktensystems. Über diese Schnittstelle werden Access Tokens für die Dokumentenverwaltung bereitgestellt und die Berechtigungen gemäß der Spezifikation in [gemSpec_Autorisierung] verwaltet. Tabelle 1.1 listet die enthaltenen logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.AUTHORIZATION.AUTHORIZE	Erteilen der Zugriffsberechtigungen an den Versicherten
LS.AUTHORIZATION.AUTHORIZATION_MANAGEMENT	Verwaltung der Zugriffsberechtigungen im Aktenkonto

Tabelle 1.1.: Logische Schnittstellen an LS.AUTHORIZATION

LS.DOCUMENT_MANAGEMENT ist die Schnittstelle des TOE zur Dokumentenverwaltung des ePA-Aktensystems. Über diese Schnittstelle werden alle Aufrufe gemäß der Schnittstellenspezifikation in [gemSpec_Dokumentenverwaltung] getätigt. Die Kommunikation ist durch den Einsatz des VAU-Protokolls abgesichert. Tabelle 1.2 listet diese logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.DOCUMENT_MANAGEMENT.CONNECT	Bereitstellung eines sicheren Kommunikationskanals zur Dokumentenverwaltung
LS.DOCUMENT_MANAGEMENT.ACCESS	Einstellen, Verwalten und Abfragen der Dokumente aus dem ePA-Aktenkonto des Versicherten
LS.DOCUMENT_MANAGEMENT.ACCOUNT	Authentisierung des Versicherten im ePA-Aktensystem

Tabelle 1.2.: Logische Schnittstellen an LS.DOCUMENT_MANAGEMENT

LS.eGK ist die Schnittstelle des TOE zur elektronischen Gesundheitskarte des Versicherten. Über diese Schnittstelle werden die in [gemSpec_Frontend_Vers], Abschnitt 6.3 aufgelisteten Aufrufe geleitet. Praktisch erfolgt eine Abbildung der eGK spezifischen TI-Plattform Befehle auf ISO-7816-4 APDUs [ISO 7816-4], die über diese Schnittstelle an die eGK versendet werden, siehe ENV_TUC_CARD_APDU_TRANSPORT in [gemSpec_SystemprozessedezTI]. Der TOE abstrahiert die Sicherheitseigenschaften des Kanals vollständig. Dieser wird für den Benutzer der API nach [gemSpec_SystemprozessedezTI] vollständig transparent. Tabelle 1.3 listet diese logischen Schnittstelle.

LS.FdV ist die Schnittstelle des TOE zur umgebenden Anwendung Frontend des Versicherten. Über diese Schnittstelle werden alle Aufrufe gemäß der Schnittstellenspezifikation aus [gemSpec_Frontend_Vers], Abschnitt 6.4.1 getätigt. Dies ist die einzige Schnittstelle, die der TOE

Bezeichner	Zweck der Schnittstelle
LS.eGK.APDU	ISO-7816-4 APDUs

Tabelle 1.3.: Logische Schnittstellen an LS.eGK

zur Verfügung stellt, die aktiv von außen benutzt wird. Gleichzeitig muss das FdV dem TOE eine Möglichkeit zur Eingabe des Authentisierungsmerkmal gegenüber der eGK zur Verfügung stellen. Dazu wird die Schnittstelle ENV_TUC_CARD_SECRET_INPUT [gemSpec_SystemprozessedezTI] verwendet. Um ausreichend Entropie zu erzeugen, muss das FdV dem TOE eine Möglichkeit zur Erzeugung von Entropie anhand einer Nutzereingabe zur Verfügung stellen. Hierfür wird dem Nutzer die Aufforderung angezeigt, über den Bildschirm zu wischen. Für die Autorisierung des FdV über OAuth mit der PKCE Erweiterung, stellt der TOE eine Schnittstelle für das Erzeugen eines code_verifiers dem FdV zur Verfügung. Tabelle 1.4 listet diese logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.FdV.API	C++ API Calls an den TOE
LS.FdV.PIN	C++ API Callback für den TOE (PIN Eingabe)
LS.FdV.ENTROPIE	C++ API Callback für den TOE zur Erzeugung von Entropie
LS.FdV.OAUTH	C++ API Callback für den TOE zur Erzeugung des PKCE code_verifiers

Tabelle 1.4.: Logische Schnittstellen an LS.FdV

LS.GATEWAY ist die Schnittstelle des TOE zum Zugangsgateway des verbundenen ePA-Aktensystems, das als Proxy zwischen dem Frontend und der Autorisierung sowie der Dokumentenverwaltung steht. Zudem setzt es die Schnittstellen zur TSL-Aktualisierung, OCSP-Prüfung und zum Verzeichnisdienst der TI um. Über die in Tabelle 1.5 aufgeführten Schnittstellen am Zugangsgateway werden alle Operationen zur Authentisierung der Versicherten und zum Zertifikatsmanagement gemäß der Schnittstellenspezifikationen [gemSpec_AuthentisierungVers] und [gemSpec_Zugangsgateway_Vers] getätigt.

Bezeichner	Zweck der Schnittstelle
LS.GATEWAY.AUTHENTICATE	Authentisierung des Versicherten im ePA-Aktensystem
LS.GATEWAY.TSL	Aktualisierung der TSL
LS.GATEWAY.OCSP	Prüfen der OCSP-Statusinformationen
LS.GATEWAY.LDAP	Zugriff auf Verzeichnisdienst der TI über LDAP-Proxy

Tabelle 1.5.: Logische Schnittstellen an LS.GATEWAY

LS.KVS ist die Schnittstelle des TOE zum Kontoverwaltungssystem über den der TOE eine al.vi beantragen und ein GdV am Signaturdienst registrieren kann. Die al.vi kann anschließend mit Hilfe des registrierten GdV über den Signaturdienst verwendet werden. Über diese Schnittstelle werden alle Aufrufe basierend auf dem OAuth2 Authorization Code Flow gemäß der Schnitt-

stellenspezifikation in [cgmKontoverwaltung_V2.3] getätigt. Tabelle 1.6 listet diese logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.KVS.AUTH_REQUEST	Authorisierung des Kontoverwaltungssystems zur Anlage einer al.vi (falls noch nicht vorhanden) und Registrierung eines GdV am Signaturdienst mit Hilfe OAuth 2.0 unter Verwendung der Erweiterung PKCE
LS.KVS.ACCESS_TOKEN_REQUEST	Anfragen eines Zugriffs-Tokens gemäß OAuth 2.0

Tabelle 1.6.: Logische Schnittstellen an LS.KVS

LS.SCHLÜSSELGENERIERUNGSDIENST ist die Schnittstelle des TOE zu den Schlüsselgenerierungsdiensten SGD1 and SGD2. Über diese Schnittstelle werden alle Aufrufe gemäß der Schnittstellenspezifikation aus [gemSpec_SGD_ePA] Abschnitt 6 getätigt.

Bezeichner	Zweck der Schnittstelle
LS.SCHLÜSSELGENERIERUNGSDIENST.GET_PUBLIC_KEY	Abrufen des öffentlichen ECIES-Schlüssels eines SGD
LS.SCHLÜSSELGENERIERUNGSDIENST.GET_AUTHENTICATION_TOKEN	Abrufen eines Authentisierungstokens
LS.SCHLÜSSELGENERIERUNGSDIENST.KEY_DERIVATION	Ableitung eines Schlüssels

Tabelle 1.7.: Logische Schnittstellen an LS.SCHLÜSSELGENERIERUNGSDIENST

LS.SECURE_STORAGE ist eine logische Schnittstelle des TOE mit dem Betriebssystem zur sicheren Speicherung von Daten. Die Schnittstelle abstrahiert dabei die Interaktion mit der Schnittstelle des OS und bietet pro Plattform drei Funktionen zum Lesen, Speichern und Löschen von Daten im sicheren Speicher des Smartphones. Die Einträge werden als Key-Value-Paar gespeichert. Tabelle 1.8 listet diese logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.SECURE_STORAGE	Lesen, Speichern und Löschen von Daten im sicheren Speicher

Tabelle 1.8.: Logische Schnittstellen an LS.SECURE_STORAGE

LS.SIGNATURDIENST ist die Schnittstelle des TOE zum Signaturdienst über den der TOE eine alternative Identität (al.vi) nutzen kann. Über diese Schnittstelle werden alle Aufrufe gemäß der Schnittstellenspezifikation in [atosAuth1_V2] getätigt. Tabelle 1.9 listet diese logischen Schnittstellen.

Bezeichner	Zweck der Schnittstelle
LS.SIGNATURDIENST.ENROLL_AUTH	Registrierung des öffentlichen Schlüssels des TOE
LS.SIGNATURDIENST.AUTH	Authentisierung des TOE geben über des Signaturdienst.
LS.SIGNATURDIENST.SIGN	Erstellung einer Signatur für die Daten des TOE mit der al.vi.
LS.SIGNATURDIENST.STAT	Abfragen über die erfolgreichen Zugriffe auf die elektronischen Identifizierungsmittel.

Tabelle 1.9.: Logische Schnittstellen an LS.SIGNATURDIENST

1.4.5. Aufbau und physische Abgrenzung des TOEs

Der TOE besteht im Kern aus in C++ geschriebener Software ergänzt um einen in Flutter umgesetzten Wrapper, der der aufrufenden GUI passende Schnittstellen bereitstellt. Der TOE unterteilt sich in drei Subsysteme: ein Subsystem „TI-Funktionalität“, das die fachliche Funktionalität des ePA Moduls kapselt, einem Subsystem „SigD-Anbindung“, dass die Kommunikation mit dem Signaturdienstund dem Kontoverwaltungssystem beinhaltet und einem Subsystem „Flutter-Plugin“ als Schnittstelle zur mit Flutter umgesetzten GUI.

1.4.6. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste

Der TOE sichert die Kommunikation zur eGK, zum Signaturdienst und KVS sowie über das Zugangsgateways des Versicherten unter anderem zum ePA-Aktensystem ab. Gleichzeitig werden die sensiblen Sessiondaten und kryptographisches Material innerhalb des TOEs geschützt, solange sie in Verwendung sind.

Der TOE überprüft insbesondere die Gültigkeit der Zertifikate des Kommunikationspartners beim Aufbau des Kanals zum ePA-Aktensystem. Zu diesem Zweck wird eine TSL (Trust-Service Status List) verwendet, welche Zertifikate von Diensteanbietern enthält. Der TOE kann anhand der aktuell gültigen TSL die Gültigkeit der Zertifikate seiner Kommunikationspartner prüfen. Um die TSL aktuell zu halten wird sie regelmäßig aktualisiert und auf Integrität und Authentizität geprüft. Außerdem überprüft der TOE, dass die verwendeten Algorithmen gültig sind.

Der TOE unterstützt demzufolge die vertrauliche und integritätsgeschützte Kommunikation mit allen Kommunikationspartnern, indem die zugehörigen kryptographischen Protokolle im TOE umgesetzt werden. Dazu gehören:

- TLS zum Zugangsgateway
- VAU-Server-Protokoll zur Dokumentenverwaltung
- ECIES-Protokoll zum Schlüsselgenerierungsdienst
- Secure Messaging mittels PACE zur eGK

- JWT über TLS zum Signaturdienst
- OAuth 2.0 über TLS mit dem Kontoverwaltungssystem

1.4.7. Physischer Umfang des TOEs

Der physische Umfang des TOEs umfasst die in Tabelle 1.10 aufgelisteten Komponenten.

Komponente	Beschreibung	Version
Software Image	Softwarepaket im git-Repository als eigentlicher TOE	v1.0.7 mit git Commit ID gemäß Guidance Documentation
Guidance Documentation („Entwicklerhandbuch“)	Die Guidance Documentation beschreibt die sichere Verwendung des TOEs.	Version gemäß Zertifizierungsreport
C++-Doxygen	Dokumentation der für den Nutzer des TOEs bereitstehenden Funktionen der C++-Bibliothek. Details zum C++-Doxygen sind der der Guidance Documentation zu entnehmen.	Version gemäß Guidance Documentation
Flutter-Doxygen	Dokumentation der für den Nutzer des TOEs bereitstehenden Funktionen des Flutter-Wrappers. Details zum Flutter-Doxygen sind der Guidance Documentation zu entnehmen.	Version gemäß Guidance Documentation
Funktionale Spezifikation	Die funktionale Spezifikation beschreibt weitere Schnittstellen, die Teil des TOEs sind, jedoch nicht durch den Nutzer des TOEs angesprochen werden und deshalb nicht in der Doxygen-Dokumentation enthalten sind.	Version gemäß Zertifizierungsreport

Tabelle 1.10.: Physischer Umfang des TOEs

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).
- CC Part 3 [CC Part 3] konform (conformant).

Es wurden funktionale Sicherheitsanforderung (FCS_RNG.1, siehe Kapitel 5.1 und FPT_EMS.1, siehe siehe Kapitel 5.2) definiert, die nicht in CC Teil 2 [CC Part 2] enthalten ist. Die Anforderungen an die Vertrauenswürdigkeit wurden ausschließlich aus CC Teil 3 [CC Part 3] entnommen.

2.2. Konformität zu Schutzprofilen

Dieses Security Target behauptet keine Konformität zu Schutzprofilen.

2.3. Konformität zu Paketen

Das Security Target strebt die Vertrauenswürdigkeitsstufe EAL2 an.

2.4. Erklärung der Konformität

Dieses Security Target behauptet erweiterte Konformität zu CC Teil 2 [CC Part 2]. Sämtliche Inhalte sind Standard-konform formuliert mit der einzigen Ausnahme der sprachlichen Anpassung von Begriffen bei der Übersetzung aus dem Englischen ins Deutsche.

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

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 abgewehrt werden müssen, welche organisatorischen Sicherheitspolitiken zu beachten sind und welche Annahmen an seine Einsatzumgebung getroffen werden müssen.

3.1. Werte

3.1.1. Zu Schützende Werte

Nutzerdaten werden im Sinne von [gemSpec_Frontend_Vers] definiert. Sie umfassen medizinische oder sonstige personenbezogene Daten einschließlich Daten des Versicherten im Verantwortungsbereich der Telematikinfrastruktur sowie Daten, die auf Anforderung des Benutzers an die Telematikinfrastruktur übergeben werden.

- *Beispiele:* alle Dokumente, die vom ePA-Aktensystem übermittelt werden, Dokumente, die der Versicherte einstellt, sonstige Versichertendaten
- *Schutzziele:* Vertraulichkeit, Integrität, Authentizität
- *Erläuterung:* Die Nutzerdaten, die vom TOE verarbeitet werden oder vom TOE an das Zugangsgateway übergeben werden bzw. in umgekehrter Richtung vom Zugangsgateway an den TOE übermittelt werden, sind zu schützen. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Zudem dürfen Daten nur zwischen authentisierten Kommunikationspartnern ausgetauscht werden.

Metadaten dienen zur Beschreibung der medizinischen Daten.

- *Beispiele:* das Erzeugungsdatum, Objektklasse oder Format- bzw. Versionsinformationen
- *Schutzziele:* Vertraulichkeit, Integrität, Authentizität
- *Erläuterung:* Die Metadaten, die von dem TOE an das Zugangsgateway übergeben werden bzw. in umgekehrter Richtung vom Zugangsgateway an den TOE übermittelt werden sind zu schützen. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Zudem dürfen Daten nur zwischen authentisierten Kommunikationspartnern ausgetauscht werden.

Sitzungsdaten werden Daten genannt, die im Sinne von Steuer- oder Ergebnisdaten im Zusammenhang mit der Verarbeitung, Speicherung oder Übertragung von Nutzerdaten und Metadaten auftreten.

- *Beispiele:* Sessiondaten die bei der Kommunikation vom ePA-Frontend mit dem ePA-Aktensystem entstehen, Konfigurationsparameter
- *Schutzziele:* Vertraulichkeit, Integrität

- *Erläuterung:* Die Metadaten, die von dem TOE an das Zugangsgateway übergeben werden bzw. in umgekehrter Richtung vom Zugangsgateway an den TOE übermittelt werden sind zu schützen. Unbefugte dürfen weder Kenntnis dieser Daten erlangen, noch diese Daten unbemerkt manipulieren können. Zudem dürfen Daten nur zwischen authentisierten Kommunikationspartnern ausgetauscht werden.

Kryptographisches Schlüsselmaterial dienen zur Umsetzung der Sicherheitsfunktionen.

- *Beispiele:* DocumentKey (AFO-ID: A_14975)
- *Schutzziele:* Vertraulichkeit, Integrität, Authentizität
- *Erläuterung:* Gelingt es einem Angreifer, Kenntnis von Schlüsselmaterial zu erlangen oder dieses zu manipulieren, so ist nicht mehr sichergestellt, dass der TOE seine Sicherheitsleistungen korrekt erbringt.

Authentisierungsmerkmale umfassen durch den TOE übertragene Verifikationsdaten. Diese werden nicht persistent gespeichert.

- *Beispiele:* PIN für eGK
- *Schutzziele:* Vertraulichkeit
- *Erläuterung:* Die Vertraulichkeit von Authentisierungsmerkmalen ist zu schützen.

TI-Vertrauensanker (TSL-Signer-CA-Zertifikat), ist die Absicherung auf Seiten des TOEs für die Authentizität der Protokollpartner für den sicheren Datenaustausch.

- *Beispiele:* TI-Vertrauensanker
- *Schutzziele:* Integrität, Authentizität
- *Erläuterung:* Gelingt es einem Angreifer, die Integrität des TI-Vertrauensankers zu verletzen, so ist nicht mehr sichergestellt, dass Nutzerdaten nicht an einen Angreifer gesendet werden.

3.1.2. Benutzer des TOE

Die *Akteure und Rollen* im Systemkontext des TOE werden in [gemSpec_Frontend_Vers, Abschnitt 3.1] beschrieben. Diese gelten unverändert für dieses Security Target, wobei aufgrund des Einschränkungen gemäß [gemSpec_FrontendVersUEePA] die Rolle des Vertreters entfällt. Des weiteren werden die folgenden Akteure bzw. Rollen ergänzt:

GUI Teil des FdV, der für den Nutzer agiert und die Funktionalität des ePA Modul FdV verwendet.

Angreifer Ein nicht legitimierter Nutzer, der Zugriff auf Versichertendaten erhalten will.

Entwickler des FdV Ein Entwickler für die übrigen, nicht TOE-Komponenten des ePA Frontends (verantwortlich u.a. für die Anwendungsoberfläche und TOE-Integration).

3.2. Bedrohungen

Der TOE muss solche Bedrohungen abwehren, die durch die Einführung der ePA-Infrastruktur neu entstehen. Bedrohungen, die auch ohne ePA-Aktensystem bestanden hätten, werden durch den TOE nicht adressiert. Dazu zählen insbesondere Bedrohungen, die durch die Ablage von Nutzerdaten durch den Versicherten lokal auf seinem Gerät entstehen. Auch bisher hatte ein Versicherter die Möglichkeit, z. B. seine medizinischen Daten zu digitalisieren und auf seinem Gerät zu speichern. Angreifer können – bei mangelhafter Absicherung des Geräts – auf die dort liegenden Daten Zugriff erlangen.

Betrachtet werden Bedrohungen der Vertraulichkeit, Integrität, Authentizität der vom TOE verarbeiteten Informationen. Es bestehen keine Verfügbarkeitsanforderungen an den TOE. Der TOE muss sicherstellen, dass er die Erfüllung der Verfügbarkeitsanforderungen an die Telematikinfrastruktur unterstützt und nicht gefährdet.

T.Mod.VA (Manipulation des Telematikinfrastruktur Vertrauensankers)
Ein Angreifer bringt einen eigenen TI-Vertrauensanker und FQDN des Gateways in den TOE ein. Dies ermöglicht ihm sein eigenes Gateway, Aktensystem und weitere TI-Systeme zu simulieren und somit an von Versicherten neu eingestellte Nutzerdaten zu gelangen.

T.Leak.PIN (Verletzung der Vertraulichkeit der Authentisierungsmerkmale der eGK)
Das Authentisierungsmerkmal für die eGK, die PIN, aber ggf. auch die PUK, kann von einem Angreifer über den TOE in Erfahrung gebracht werden. Dies schwächt die Sicherheit der Zwei-Faktor-Authentifizierung mittels eGK.

T.Tamper.eGK (Integrität und Vertraulichkeit der Kommunikation zur eGK)
Ein Angreifer hört Daten ab oder manipuliert Daten, die zwischen dem TOE und der eGK des Versicherten übertragen werden. Dies umfasst unter anderem auch passives Sniffen und dass ein Angreifer verschlüsselte Daten während der Übertragung unbemerkt verändert.

T.Leak.Config (Vertraulichkeit von persistent gespeicherten Konfigurationsdaten)
Eine Anwendung auf dem GdV liest persistent gespeicherte, schützenswerte Daten und Konfigurationsparameter (z.B. Geräteidentifikator) aus dem Gerät aus.

T.Leak.Session (Vertraulichkeit von nicht-persistent gespeicherten Schlüsselinformationen)
Nicht persistent gespeicherte Schlüsselinformationen werden von einer Anwendung auf dem GdV aus dem Speicher gelesen.

T.Leak.Key (Vertraulichkeit von persistent gespeicherten Schlüsselinformationen)
Persistent gespeicherte Schlüsselinformationen für die Authentifizierung gegenüber dem Signaturdienst werden von einer unautorisierten Anwendung auf dem GdV ausgelesen.

3.3. Organisatorische Sicherheitspolitiken

OSP.Komm.GW (Sichere Kommunikation mit dem Zugangsgateway)
Der TOE kommuniziert mit dem Zugangsgateway nur über einen mit TLS abgesicherten Kanal.

OSP.Komm.DocMgmt (Sichere Kommunikation mit der Dokumentenverwaltung)
Der TOE kommuniziert mit der Dokumentenverwaltung nur über einen mit dem in [gemSpec_Krypt] spezifizierten VAU-Protokoll abgesicherten Kanal.

OSP.Komm.SGD (Sichere Kommunikation mit dem Schlüsselgenerierungsdienst)
Der TOE kommuniziert mit der Schlüsselgenerierungsdienst nur über einen mit dem in [gemSpec_Krypt] spezifizierten ECIES-Protokoll abgesicherten Kanal.

OSP.Komm.KVS (Sichere Kommunikation mit dem Kontoverwaltungssystem)
Der TOE kommuniziert mit dem Kontoverwaltungssystem nur über einen mit TLS abgesicherten Kanal. Der TOE verwendet OAuth 2.0 innerhalb der TLS-Verbindung um sich gegenüber dem Kontoverwaltungssystem zu authentifizieren.

OSP.Komm.SigD (Sichere Kommunikation mit dem Signaturdienst)
Der TOE kommuniziert mit dem Signaturdienst nur über einen mit TLS abgesicherten Kanal. Der TOE authentifiziert seine Nachrichten innerhalb des TLS-Kanal mit JWS.

OSP.Dok.Verschl (Schutz der Dokumente)
Der TOE unterstützt die Verschlüsselung der Dokumente in der Dokumentenverwaltung um diese gegen unbefugten Zugriff vom Aktensystem abzusichern. Dazu kommt die symmetrische Verschlüsselung aus [gemSpec_Krypt] zum Einsatz. Gleichzeitig wird auch die Erstellung sämtlicher dazu benötigter Schlüssel vom TOE gefordert.

OSP.KryptAlgo (Kryptographische Algorithmen)
Alle kryptographischen Sicherheitsmechanismen der technischen Komponenten der Telematikinfrastruktur werden im Einklang mit den relevanten Vorgaben des Dokuments BSI TR-03116-1 [TR-03116-1] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [gemSpec_Krypt] implementiert.

OSP.Entropy (Starke Zufallsquelle)
Ein nicht mit ausreichend Entropie geseedeter Zufallswertgenerator, generiert Zufallswerte, die die eingesetzte Kryptographie schwächen. Es muss eine Zufallsquelle verwendet werden, die den Anforderungen der gematik aus [gemSpec_Krypt] entspricht.

3.4. Annahmen

A.Secure.TI (Sichere Telematikinfrastruktur-Plattform)
Die zentrale Telematikinfrastruktur-Plattform, insbesondere das Zugangsgateway, wird als vertrauenswürdig angesehen, d. h. Angriffe aus der zentralen TI-Plattform sowie aus Netzen, die mit der zentralen TI-Plattform verbunden sind, werden nicht betrachtet. Die Betreiber der Telematikinfrastruktur sorgen dafür, dass die Telematikinfrastruktur frei von Schadsoftware gehalten wird, so dass über den sicheren Kommunikationskanal hinein keine Angriffe erfolgen. Dies beinhaltet neben Zugangsgateway insbesondere auch den Schlüsselgenerierungsdienst. Die kryptografischen Schlüssel auf Seiten der TI-Plattform werden geheim gehalten und sind nur für die rechtmäßigen Administratoren zugänglich. Schlüsselmaterial wird nicht durch Angreifer entwendet. Alle Administratoren in der Telematikinfrastruktur sind fachkundig und vertrauenswürdig.

A.Secure.eGK (Sichere eGK)
Das Authentifizierungsverfahren mittels eGK wird als vertrauenswürdig angenommen, d. h. Angriffe von der eGK aus werden nicht betrachtet. Die schließt auch Angriffe durch eine potentiell gefälschte eGK aus. Ein Angreifer könnte damit die Zufallsquelle schwächen. Dies lässt sich aber im weiteren

Verlauf nicht ausnutzen, da vor Etablierung des VAU-Server-Protokoll geschützten Kanals zur Dokumentenverwaltung die Authentizität der Karte kryptographisch überprüft wird.

A.Secure.KVS (Sicheres Kontoverwaltungssystem)
Der Betreiber des Kontoverwaltungssystem muss sicherstellen, dass vom Kontoverwaltungssystem aus keine Angriffe gegen den TOE durchgeführt werden.

A.Secure.SigD (Sicherer Signaturdienst)
Die Betreiber und Aussteller des Signaturdienstes müssen sicherstellen, dass vom Signaturdienst aus keine Angriffe gegen das ePA Modul FdV durchgeführt werden.

A.Correct.GUI (Korrekte TOE-Nutzung durch FdV)
Die Anwendung Frontend des Versicherten auf dem Gerät des Versicherten übergibt die Daten, die durch Dienste gemäß § 291a SGB V verarbeitet werden sollen, in korrekter Weise an den TOE, damit der TOE zu schützende Daten einem Aktensystem über den entsprechenden abgesicherte Kanäle versenden kann. Dazu verwendet die Anwendung die vom TOE bereitgestellten Schnittstellen dermaßen, dass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

A.NonMalicious.Dev (Nicht böswilliger FdV-Entwickler)
Alle Entwickler des FdV sind fachkundig und vertrauenswürdig. Sie binden den TOE gemäß Spezifikation in das FdV ein, konfigurieren es korrekt, verletzen nicht die Integrität der TOE-Software und fügen insbesondere keine unerlaubten Nebenfunktionen hinzu.

A.Secure.Device (Sichere Verwaltung GdV)
Das GdV ist nach aktuellen Stand der Technik entwickelt worden und der Anwender administriert das Gerät auf sichere Art und Weise. Der Anwender hält sein Gerät in einem aktuellen und vertrauenswürdigen Zustand. Zusätzlich setzt das GdV entsprechend den Angaben des Herstellers des GdV Sicherheitseigenschaften um.

A.Integr.FdV (Integrität des FdV)
Das FdV nutzt die Sicherheitsleistungen der Plattform (Betriebssystem). Dies beinhaltet eine kryptographische Überprüfung der Integrität des FdV und somit auch des TOE in seiner Gesamtheit bei jedem Start.

4. Sicherheitsziele

4.1. Sicherheitsziele des TOE

4.1.1. Generelle Schnittstellen

0.TLS.Krypto (TLS-Kanäle mit sicheren kryptographischen Algorithmen)
Der TOE setzt TLS-Kanäle zur Gewährleistung der Integrität, Authentizität und Vertraulichkeit der Kommunikation mit anderen IT-Produkten ein. Er verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [TR-03116-1] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [gemSpec_Krypt]. Zudem prüft der TOE die Gültigkeit der Zertifikate, die für den Aufbau eines TLS-Kanals verwendet werden.

4.1.2. Schnittstelle zur Dokumentenverwaltung

0.VAU (VAU-Protokoll zur sicheren Kommunikation mit der Dokumentenverwaltung)
Der TOE setzt das VAU-Protokoll zur Gewährleistung der Integrität und Vertraulichkeit während der Kommunikation mit der Dokumentenverwaltung ein. Das Protokoll wird in Kapitel 6 der übergreifenden Spezifikation: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt] spezifiziert.

4.1.3. Schnittstelle zum Schlüsselgenerierungsdienst

0.ECIES (ECIES-Protokoll zur sicheren Kommunikation mit dem Schlüsselgenerierungsdienst)
Der TOE setzt das ECIES-Verfahren zur Gewährleistung der Integrität und Vertraulichkeit der Kommunikation mit dem Schlüsselgenerierungsdienst ein. Er verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [gemSpec_Krypt] und [gemSpec_SGD_ePA].

4.1.4. Schnittstelle zur eGK

0.eGK.SM (Secure Messaging Kanal zur eGK)
Der TOE setzt zur Gewährleistung der Integrität und Vertraulichkeit der Kommunikation mit der eGK Secure Messaging ein. Er verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [gemSpec_COS].

4.1.5. Schnittstelle zum Kontoverwaltungssystem

0.OAUTH (Autorisierung des Kontoverwaltungssystem)
Der TOE verwendet OAuth in Version 2.0 mit der PKCE Erweiterung gemäß [RFC 6749] und [RFC 7636] beschrieben in [cgmKontoverwaltung_V2.3] für die Beantragung einer al.vi und Registrierung eines neuen GdVs.

4.1.6. Schnittstelle zum Signaturdienst

O.JWS (Authentifizierung der übertragenen Daten)
Der TOE setzt JSON Web Signature (JWS) zur Gewährleistung der Authentizität der ausgetauschten Daten ein. Er verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [TR-03107-1] mit den Einschränkungen der AtoS Dokumentation für Kryptoalgorithmen [atosAuth1_V2].

4.1.7. Schnittstelle zum Gerät des Versicherten

O.Secure.Storage (Vertrauliche Speicherung von Daten)
Der TOE speichert automatisch nur dann schützenswerte Daten und Konfigurationsparameter persistent, wenn dies für die Funktionsfähigkeit des TOEs gemäß Spezifikation notwendig ist. Zur Ablage von persistent zu speichernden Daten, wird der vom GdV und dessen Betriebssystem zur Verfügung gestellte sicheren Speicher verwendet. Unter anderem wird der private Schlüssel der al.vi in diesem Speicher abgelegt und kann nicht exportiert werden.

4.1.8. Kryptographische Sicherheitsziele

O.Basis.Krypto (Kryptographische Algorithmen)
Der TOE verwendet sichere kryptographische Algorithmen und Protokolle für alle Kryptoverfahren gemäß [TR-03116-1] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [gemSpec_Krypt].

O.RNG (Zufallszahlengenerator)
Der TOE verwendet einen Zufallszahlengenerator, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klasse DRG.3 liefert.

4.1.9. Übergreifende Sicherheitsziele

O.Schutz.Mem (Schutz von Sitzungsdaten)
Der TOE schützt die zur Laufzeit ihm übergebenen und im TOE entstehenden Daten, unabhängig von ihrer persistenten Speicherung sofern anwendbar. Zu diesen Daten gehören die Authentisierungsmerkmale, die Sitzungsdaten und kryptographisches Schlüsselmaterial. Der TOE löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden. Diese Daten werden auch nur über die Schnittstellen ausgegeben, über die sie nach der Spezifikation des TOEs ausgegeben werden müssen.

O.Dok.Verschl (Dokumentenverschlüsselung)
Der TOE stellt (medizinische) Dokumente des Versicherten nur symmetrisch verschlüsselt in die Dokumentenverwaltung ein. Der zugehörige Dokumentenschlüssel wird mit dem Aktenschlüssel verschlüsselt in der Dokumentenverwaltung hinterlegt. Akten- und Kontextschlüssel werden den Schlüsselgenerierungsdiensten übergeben. Die Verschlüsselung und die Schlüsselerzeugung erfolgt nach den Maßgaben aus [gemSpec_Krypt].

4.2. Sicherheitsziele für die Umgebung des TOE

OE.Secure.TI (Sichere Telematikinfrastruktur-Plattform)
Die Betreiber der zentralen Telematikinfrastruktur-Plattform müssen sicherstellen, dass aus dem Netz der zentralen TI-Plattform und von den Komponenten der TI heraus keine Angriffe gegen den TOE durchgeführt werden.

OE.Secure.eGK (Sichere eGK)
Der Versicherte als Inhaber der eGK und der Aussteller der eGK müssen sicherstellen, dass von der eGK aus keine Angriffe gegen den TOE durchgeführt werden.

OE.Secure.KVS (Sicheres KVS)
Die Betreiber der Kontoverwaltungssystem-Infrastruktur müssen sicherstellen, dass vom Kontoverwaltungssystemaus keine Angriffe gegen den TOE durchgeführt werden.

OE.Secure.SigD (Sicherer SigD)
Die Betreiber und Aussteller des Signaturdienstes müssen sicherstellen, dass vom Signaturdienst aus keine Angriffe gegen den TOE durchgeführt werden.

OE.KeyStorage (Vertrauenswürdiger Schlüsselspeicher)
Das GdV stellt dem TOE einen sicheren Schlüsselspeicher bereit. Der sichere Schlüsselspeicher schützt sowohl die Vertraulichkeit, als auch die Integrität des in ihm gespeicherten Schlüsselmaterials.

OE.Correct.GUI (Korrekte TOE-Nutzung durch FdV)
Die Anwendung Frontend des Versicherten auf dem Gerät des Versicherten muss die Daten, die durch Dienste gemäß § 291a SGB V verarbeitet werden sollen, in korrekter Weise an den TOE übergeben, damit der TOE zu schützende Daten einem Aktensystem über den entsprechenden abgesicherte Kanäle versenden kann. Dazu muss die Anwendung die vom TOE bereitgestellten Schnittstellen geeignet verwenden, so dass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

OE.NonMalicious.Dev (Nicht böswilliger FdV-Entwickler)
Alle Entwickler des FdV müssen fachkundig und vertrauenswürdig sein. Sie müssen den TOE gemäß Spezifikation in das FdV einbinden, korrekt konfigurieren und dürfen die Integrität der TOE-Software nicht verletzen und keine unerlaubten Nebenfunktionen hinzufügen.

OE.Secure.Device (Sichere Verwaltung GdV)
Das GdV muss nach aktuellen Stand der Technik entwickelt worden sein. Der Anwender muss das Gerät auf sicherer Art und Weise administrieren. Es obliegt der Sorgfaltspflicht des Anwenders sein Gerät in einem aktuellen und vertrauenswürdigen Zustand zu halten.

OE.Integr.FdV (Schutz des TI-Vertrauensankers)
Das FdV schützt sich gegen Manipulation des TI-Vertrauensankers durch eine Überprüfung der Integrität und Authentizität des TI-Vertrauensankers bei jedem Start.

4.3. Erklärung der Sicherheitsziele des TOE

In diesem Abschnitt wird der Nachweis geführt, dass die oben formulierten und in Tabelle 4.1 auf die Bedrohungen abgebildeten Sicherheitsziele geeignet sind, um die Bedrohungen abzuwehren.

	O.Basis.Krypto	O.eGK.SM	O.ECIES	O.VAU	O.Secure.Storage	O.Dok.Verschl	O.TLS.Krypto	O.OAUTH	O.Schutz.Mem	O.RNG	O.JWS	OE.KeyStorage	OE.Secure.TI	OE.Secure.eGK	OE.Secure.KVS	OE.Secure.SigD	OE.Correct.GUI	OE.NonMalicious.Dev	OE.Secure.Device	OE.Integr.FdV
T.Tamper.eGK	.	✓	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	✓	.	.
T.Leak.Config	.	.	.	.	✓	.	.	.	✓	.	.	✓	.	.	.	.	.	✓	✓	.
T.Leak.PIN	.	✓	.	.	.	.	.	.	✓	.	.	.	.	✓	.	.	✓	✓	✓	.
T.Leak.Session	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	✓	.	.
T.Leak.Key	.	.	.	.	✓	.	.	.	.	.	.	✓	.	.	.	.	.	✓	✓	.
T.Mod.VA	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	✓	✓
OSP.Komm.GW	.	.	.	.	.	.	✓	.	.	.	.	.	✓	.	.	.	.	✓	.	.
OSP.Komm.DocMgmt	.	.	.	✓	.	.	.	.	.	.	.	.	✓	.	.	.	.	✓	.	.
OSP.Komm.SGD	.	.	✓	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	✓	.	.
OSP.Komm.KVS	.	.	.	.	.	.	✓	✓	.	.	.	.	.	.	✓	.	.	✓	.	.
OSP.Komm.SigD	.	.	.	.	.	.	✓	.	.	.	✓	.	.	.	.	✓	.	✓	.	.
OSP.Dok.Verschl	.	.	.	.	.	✓	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
OSP.KryptAlgo	✓	.	.	.	.	.	✓	.	.	✓	.	.	.	.	.	.	.	✓	.	.
OSP.Entropy	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.	✓	.	.
A.Secure.TI	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.	.
A.Secure.eGK	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.	.
A.Secure.KVS	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.	.
A.Secure.SigD	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.	.
A.Correct.GUI	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.	.
A.NonMalicious.Dev	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.	.
A.Secure.Device	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓	.
A.Integr.FdV	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	✓

Tabelle 4.1.: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen

4.3.1. Abwehr der Bedrohungen durch die Sicherheitsziele

4.3.1.1. T.Tamper.eGK

O.eGK.SM gewährleistet, dass das ein Secure Messaging Kanal zur Kommunikation mit der eGK eingesetzt wird. Dies gewährleistet insbesondere die Erfüllung der Anforderungen an die Vertraulichkeit und Integrität der Kommunikation. OE.Secure.eGK gewährleistet die selben Schutzziele auf Seite der eGK. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zur eGK nur über den TOE hergestellt wird.

4.3.1.2. T.Leak.Config

Für schützenswerte Daten und Konfigurationsparameter, die gespeichert werden müssen, gewährleistet O.Secure.Storage in Verbindung mit OE.KeyStorage, dass ein sicherer Speicher auf dem Gerät vorhanden ist und verwendet wird. OE.Secure.Device gewährleistet, dass die vorhandene Sicherheit nicht durch inkorrekte Administration gefährdet wird. So wird insgesamt der Schutz der Vertraulichkeit der gespeicherten schützenswerten Daten und Konfigurationsparameter gewährleistet. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und Konfigurationsparameter nicht außerhalb der Kontrolle des TOEs gespeichert werden. O.Schutz.Mem gewährleistet, dass die Konfigurationsparameter auch bei der Verarbeitung im TOE geschützt sind, und dass sie nur über die dafür vorgegebenen Schnittstellen den TOE verlassen.

4.3.1.3. T.Leak.PIN

O.Schutz.Mem gewährleistet, dass das Authentisierungsmerkmal (PIN) für die eGK nicht persistent gespeichert werden und damit auch nicht aus dem persistenten Speicher ausgelesen werden kann sowie, dass sie nur über die dafür vorgegebene Schnittstelle zur eGK den TOE verlässt. O.eGK.SM gewährleistet, dass das ein Secure Messaging Kanal zur Kommunikation mit der eGK eingesetzt wird. Dies gewährleistet insbesondere die Erfüllung der Anforderungen an die Vertraulichkeit des Authorisierungsmerkmals, wenn dieses bei einer PIN-Management-Operation an die eGK übertragen wird. OE.Secure.eGK gewährleistet die selben Schutzziele auf Seite der eGK. OE.Correct.GUI und OE.Secure.Device gewährleisten die Vertraulichkeit der PIN bei der Eingabe auf dem GdV mittels des FdV. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und Authentisierungsmerkmale nicht außerhalb des TOEs verwendet werden, abgesehen von der Eingabe für die Verwendung im TOE.

4.3.1.4. T.Leak.Session

O.Schutz.Mem gewährleistet den Schutz der Vertraulichkeit von nicht-persistent gespeicherten Daten durch sofortiges Löschen und aktives Überschreiben, indem Geheimnisse nach Benutzung aktiv gelöscht werden. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Sitzungsdaten nur im TOE anfallen.

4.3.1.5. T.Mod.VA

OE.Integr.FdV gewährleistet die Erkennung von Modifikationen des TI-Vertrauensankers mittels Erkennung von Modifikationen am FdV durch Sicherheitsrichtlinien der Plattform. OE.Secure.Device erfordert, dass das GdV sicher verwaltet wird. Dies soll einen Angreifer keine einfache Möglichkeit einräumen, den TI-Vertrauensanker im TOE zu modifizieren bzw. die Sicherheitsrichtlinien der Plattform zu

umgehen. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und eine Veränderung des TI-Vertrauensankers durch den Entwickler ausgeschlossen wird.

4.3.1.6. T.Leak.Key

Für persistent gespeicherte kryptographische Schlüssel gewährleistet O.Secure.Storage in Verbindung mit OE.KeyStorage, dass ein sicherer Speicher auf dem Gerät vorhanden ist und verwendet wird. OE.Secure.Device gewährleistet, dass die vorhandene Sicherheit nicht durch inkorrekte Administration gefährdet wird. So wird insgesamt der Schutz der Vertraulichkeit der gespeicherten schützenswerten Schlüssel gewährleistet. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und Schlüsselmaterial aus dem TOE nur im TOE verbleibt.

4.3.2. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

4.3.2.1. OSP.Komm.GW

Die Gewährleistung der Authentizität des GW ist die notwendige Voraussetzung für die Sicherstellung der Vertraulichkeit in der Kommunikation mit dem GW.

O.TLS.Krypto verifiziert das Zertifikat für die Authentizität des Zugangsgateways und schützt die Integrität, Authentizität und Vertraulichkeit der Verbindung zum Zugangsgateway durch den Einsatz von Kryptographie in Form von TLS. OE.Secure.TI gewährleistet die selben Schutzziele auf Seite des Zugangsgateways. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zum Zugangsgateway nur über den TOE hergestellt wird.

4.3.2.2. OSP.Komm.SGD

O.ECIES gewährleistet die Erfüllung der Anforderungen an die Vertraulichkeit und Integrität der Kommunikation sowie an die Authentizität durch die Umsetzung des ECIES-Protokolls. OE.Secure.TI gewährleistet die selben Schutzziele auf Seiten der Schlüsselgenerierungsdienste. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zu den Schlüsselgenerierungsdiensten nur über den TOE hergestellt wird.

4.3.2.3. OSP.Komm.DocMgmt

O.VAU gewährleistet die Erfüllung der Anforderungen an die Vertraulichkeit und Integrität der Kommunikation sowie an die Authentizität durch die Umsetzung des VAU-Server-Protokolls. OE.Secure.TI gewährleistet die selben Schutzziele auf Seite der Dokumentenverwaltung. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zur Dokumentenverwaltung nur über den TOE hergestellt wird.

4.3.2.4. OSP.Komm.KVS

O.TLS.Krypto gewährleistet die Erfüllung der Anforderungen an die Vertraulichkeit und Integrität der Kommunikation sowie an die Authentizität des Kontoverwaltungssystem gegenüber des TOE. O.OAUTH Authentifzeirt den TOE gegenüber dem Kontoverwaltungssystem. OE.Secure.KVS gewährleistet die selben Schutzziele auf Seite des KVS. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zum KVS nur über den TOE hergestellt wird.

4.3.2.5. OSP.Komm.SigD

O.TLS.Krypto gewährleistet die Erfüllung der Anforderungen an die Vertraulichkeit und Integrität der Kommunikation sowie an die Authentizität des Signaturdienst gegenüber dem TOE. O.JWS gewährleistet die Erfüllung der Anforderung der Authentizität des TOEs gegenüber dem Signaturdienst. OE.Secure.SigD gewährleistet die entsprechenden Schutzziele auf Seite des Signaturdiensts. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Verbindung zum Signaturdienst nur über den TOE hergestellt wird.

4.3.2.6. OSP.Dok.Verschl

O.Dok.Verschl gewährleistet die Erfüllung der Anforderungen an die Vertraulichkeit der medizinischen Nutzerdokumente zum Schutz gegen Zugriff aus dem Aktensystem durch Umsetzung der Dokumentenverschlüsselung. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und die Nutzerdokumente nicht ohne Absicht des Nutzers exportiert werden.

4.3.2.7. OSP.KryptAlgo

O.Basis.Krypto setzt die Richtlinie zur Nutzung von Kryptographie um. Die geforderten Spezifikationen werden in O.TLS.Krypto und O.RNG aufgegriffen. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und für alle kryptographischen Operationen nur der TOE verwendet wird.

4.3.2.8. OSP.Entropy

O.RNG stellt sicher, dass Zufallszahlen ausreichender Güte verwendet werden. OE.NonMalicious.Dev gewährleistet, dass der TOE wie spezifiziert verwendet wird, und dass die für die Generierung des Zufalls nötigen Eingangsdaten korrekt an den TOE übergeben werden.

4.3.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Bei den folgenden inhaltlich lediglich umformulierten Annahmen (A....) bzw. Umgebungszielen (OE....) besteht eine direkte Eins-zu-eins-Beziehung.

4.3.3.1. A.Secure.TI

OE.Secure.TI bildet direkt A.Secure.TI ab.

4.3.3.2. A.Secure.eGK

OE.Secure.eGK bildet direkt A.Secure.eGK ab.

4.3.3.3. A.Secure.KVS

OE.Secure.KVS bildet direkt A.Secure.KVS ab.

4.3.3.4. A.Secure.SigD

OE.Secure.SigD bildet direkt A.Secure.SigD ab.

4.3.3.5. A.Correct.GUI

OE.Correct.GUI bildet direkt A.Correct.GUI ab.

4.3.3.6. A.NonMalicious.Dev

OE.NonMalicious.Dev bildet direkt A.NonMalicious.Dev ab.

4.3.3.7. A.Secure.Device

OE.Secure.Device bildet direkt A.Secure.Device ab.

4.3.3.8. A.Integr.FdV

OE.Integr.FdV bildet direkt A.Integr.FdV ab.

5. Definition der erweiterten Komponenten

In diesem Kapitel werden die Familien der erweiterten Sicherheitsanforderungen für das Erzeugen von Zufallszahl und dem Einschränken der Ausgabe schützenswerter Daten beschrieben. Erweiterte Sicherheitsanforderungen an die Vertrauenswürdigkeit werden nicht hinzugefügt.

5.1. Definition der erweiterten Familie FCS_RNG

Familienverhalten

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Komponentenabstufung

FCS_RNG	Generation of random numbers	1

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1
Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependnencies.
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 den Anforderungen in [gemSpec_Frontend_Vers] in Verbindung mit [gemSpec_Krypt] ist der TOE für die Zulieferung von Zufallszahlen verantwortlich.

5.2. Definition der erweiterten Familie FPT_EMS

Familienverhalten

This family defines requirements to mitigate intelligible emanations.

Komponentenabstufung

FPT_EMS	TOE Emanation	1

FPT_EMS.1 Emanation of TSF and User data, defines limits of TOE emanation related to TSF and User data.

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

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

FPT_EMS.1
Emanation of TSF and User data

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
FPT_EMS.1.2	The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Erklärung für die Einführung der erweiterten Familie

Diese Familie wurde ursprünglich eingeführt, um die elektromagnetische Abstrahlung als Seitenkanal explizit zu betrachten. In diesem Security Target wird diese Familie in geänderter Interpretation verwendet, um die Ausgabe von schützenswerten Daten über die Schnittstellen des TOEs einzuschränken.

6. Sicherheitsanforderungen

6.1. Hinweise und Definitionen

6.1.1. Hinweise zur Notation

Die Auswahl der funktionalen Sicherheitsanforderungen basiert auf der zum Zeitpunkt der Erstellung des Security Targets aktuellen Version 3.1 Revision 5 der Common Criteria; diese Version [CC Part 2] liegt in englischer Sprache vor. Diese wurden in diesem Security Target übernommen.

Die Common Criteria erlauben die Anwendung verschiedener Operationen auf die funktionalen Sicherheitsanforderungen; Zuweisung, Auswahl, Verfeinerung und Iteration.

Die typographischen Auszeichnungen für die Operationen an den SFR sind in Tabelle 6.1 beschrieben.

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

Tabelle 6.1.: Typographische Konventionen

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Die im Folgenden genannten Daten stammen direkt aus der Spezifikation des ePA Frontend des Versicherten [gemSpec_Frontend_Vers] Kapitel 7, Informationsmodell. Für etwaige, nicht eingeführte Abkürzungen und Akronyme sei auf die Quelle verwiesen.

6.1.2.1. Subjekte

Nutzer Identifikator des Nutzers, in dessen Auftrag das ePA Modul FdV agiert. Das einzige Subjekt des TOE. Dieses Subjekt wird durch die Daten in Tabelle 6.2 repräsentiert. In der technischen Betrachtung interagiert der Nutzer mit der GUI (dem FdV).

6.1.2.2. Objekte

Aktenkonto Identifiziert ein konkretes Aktenkonto in einem ePA-Aktensystem. Die Daten sind in Tabelle 6.3 aufgelistet. Diese werden im ePA Frontend des Versicherten persistent vorgehalten und dem ePA Modul FdV bei den entsprechenden Aufrufen übergeben.

Datenfeld	Beschreibung
Authentisierungszertifikat des Nutzers	falls eGK: C.CH.AUT; falls alternative kryptographische Versichertenidentität: C.CH.AUT_ALT
Name des Nutzers	
Versicherten-ID des Nutzers	
Benachrichtigungskanal für Geräteverwaltung (E-Mail)	durch den Nutzer während des Eröffnens des Aktenkontos angegeben.

Tabelle 6.2.: Datenfelder Nutzer

Datenfeld	Beschreibung
Akten-ID	beinhaltet Versicherten-ID und Anbieter-ID (homeCommunityId)
Name des Aktenkontoinhabers	
FQDN des Aktensystems	

Tabelle 6.3.: Datenfelder Aktenkonto

Berechtigungen Sicherheitsattribute des Aktensystems, aber reines Datum für das epa-Modul des FdV. Die Daten sind in Tabelle 6.4 aufgelistet. Diese werden nicht persistiert.

Gerätedaten Identifizieren ein GdV eindeutig. Die Daten sind in Tabelle 6.5 aufgelistet. Diese werden im TOE persistent gespeichert.

Gerätedaten Signaturdienst Identifizieren ein GdV gegenüber dem Signaturdienst eindeutig. Die Daten sind in Tabelle 6.6 aufgelistet. Diese werden im TOE persistent gespeichert.

Nutzerdaten Nutzerdaten werden im Sinne von [gemSpec_Frontend_Vers] definiert. Sie umfassen medizinische oder sonstige personenbezogene Daten einschließlich Daten des Versicherten im Verantwortungsbereich der Telematikinfrastruktur sowie Daten, die auf Anforderung des Benutzers an die Telematikinfrastruktur übergeben werden.

Metadaten Metadaten zu den Nutzerdaten. Sie dienen zur Beschreibung der medizinischen Daten.

Konfigurationsdaten Persistent zu speichernde Daten des ePA Modul FdV. Die Daten sind in Tabelle 6.7 aufgelistet.

PIN Authentisierungsmerkmal gegenüber der eGK. Je nach Anwendungsfall wird das Authentisierungsmerkmal zur Erstellung eines sicheren Kanals verwendet, oder innerhalb des sicheren Kanales zur Karte übertragen. Die PIN steht hier symbolisch für alle auf der eGK verwendeten Authentisierungsmerkmale PIN und PUK. Das Merkmal PUK kommt nur beim Anwendungsfall des PIN-Managements zum Einsatz.

AktenID (RecordIdentifier) Kennung des Aktenkontos, auf das in der Aktensession zugegriffen wird, im Format von RecordIdentifier gemäß [gemSpec_DMePA]. Die homeCommunityID muss bekannt sein.

Datenfeld	Beschreibung
Name des Berechtigten	
Kategorie	LEI , KTR oder Vertreter
ID	für LEI oder KTR: Telematik-ID für Vertreter: Versicherten-ID
Berechtigung ausgestellt am	nur LEI
Berechtigung gültig bis	nur LEI
Berechtigung für den Zugriff von LEI eingestellten Dokumenten	nur LEI
Berechtigung für den Zugriff von Versicherten eingestellten Dokumenten	nur LEI
Berechtigung für den Zugriff von KTR eingestellten Dokumenten	nur LEI

Tabelle 6.4.: Datenfelder Berechtigungen

Datenfeld	Beschreibung
Gerätekennung	beinhaltet Gerätenamen und Geräteidentität
Geräteidentität (DeviceID)	wird von der Autorisierung beim erstmaligen Aufruf zusammen mit dem DEVICE_UNKNOWN Fehler übermittelt
Gerätenamen	durch Nutzer festgelegt

Tabelle 6.5.: Datenfelder Gerätedaten

Datenfeld	Beschreibung
Geräteidentität (DeviceID)	ID zur Geräte Identifikation, wird von Kontoverwaltungssystem bei Registrierung des GdV ausgestellt
KVNR	Krankenversichertennummer des Versicherten
KHG	Mandanten-ID des Signaturdienstes für die Krankenkasse

Tabelle 6.6.: Datenfelder Gerätedaten Signaturdienst nach [atosAuth1_V2]

Parameter	Beschreibung
Aktenkontoinhaber: Akten-ID	Akten-ID (RecordIdentifier) des Aktenkontos für den Versicherten
Aktenkontoinhaber: Anbieter-ID	„HomeCommunityId“ des ePA-Aktensystems. Der Parameter wird mittels Abfrage des Namensdienstes im Internet bestimmt. Er wird durch das FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.
Aktenkontoinhaber: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den Versicherten
Aktenkontoinhaber: Geräteidentifikator	Von der Autorisierung einmalig übermittelte Zufallszahl. Wird durch das ePA-Modul FdV übernommen und ist nicht durch den Nutzer konfigurierbar. Der Parameter wird nicht angezeigt.
Aktenkontoinhaber: Letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Logins des Nutzers in das Aktenkonto von dem Gerät. Dient der Auswahl der Benachrichtigungen; Der Parameter wird durch das ePA-Modul FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.
Benachrichtigungen aktivieren	Benachrichtigung über neue, geänderte oder gelöschte ePA-Dokumente
Benachrichtigungszeitraum	
Dokumente einstellen: Berechtigte anzeigen	gibt an, ob im Anwendungsfall Dokumente einstellen die Liste der für den Zugriff Berechtigten vor dem Hochladen angezeigt wird.
Gerätenamen	Bezeichnung des GdV durch den Nutzer, um es im Freischaltprozess und während der Geräteverwaltung leichter wiedererkennen zu können. Bildet zusammen mit dem Geräteidentifikator die Gerätekennung (DeviceID). Die Gerätekennung wird für die Geräteautorisierung genutzt.

Tabelle 6.7.: Konfigurationsdaten

Status Nutzer (Aktenkontoinhaber oder Vertreter) Vergleich Versicherten-ID aus Akten-ID mit Versicherten-ID aus Authentisierungszertifikat des Nutzers.

Liste der vergebenen Berechtigungen Liste der für alle Berechtigungen ausgelesenen AuthorizationKeys und Policy Documents.

Authentisierungstoken (AuthenticationAssertion) Authentifizierungsbestätigung

Autorisierungstoken (AuthorizationAssertion) Autorierungsbestätigung

Zustand des Aktenkontos (RecordState) Zeitpunkt der letzten Authentifizierung durch den Nutzer.

6.1.2.2.1. TSF-Daten

Es gibt nur wenige persistente TSF-Daten. Das sind der TI-Vertrauensanker in Form eines TSL-Signer-CA-Zertifikat (Trust Service Status List), die fest mit dem Code des TOEs verbunden ist, und das Schlüsselpaar zur Authentifizierung gegenüber dem Signaturdienst.

TI-Vertrauensanker - TSL-Signer-CA-Zertifikat CA Zertifikat zur Prüfung gültiger Telematikinfrastruktur-Zertifikate.

TSL Trust-Service Status List enthält die Zertifikate der Diensteanbieter. Dient zur Prüfung der Zertifikate der Telematikinfrastruktur.

SigD-Schlüsselpaar Persistent zu speicherndes Schlüsselpaar des TOEs für die Authentisierung gegenüber dem Signaturdienst.

Zustand des DRNG Abgespeicherter, interner Zustand des DRNG

Daneben werden TSF-Daten von der Umgebung bereitgestellt.

TLS CA-Zertifikate X.509 CA Zertifikate für Internet Verbindungen auf Basis von TLS.

Es gibt eine Reihe von Daten, die im Laufe der Sitzungserstellung anfallen. Diese werden für die Dauer der Sitzung gehalten, bei Abbau der Sitzung sofort freigegeben.

ECIES-Protokoll Sitzungsschlüssel Ephemerale Schlüssel der ECIES-Protokollsitzung mit dem Schlüsselgenerierungsdienst.

RegistrationToken Vom Signaturdienst ausgestelltes Anmeldetoken.

Prüfcode Zufällig erzeugter Prüfcode zur Identifizierung gegenüber dem Kontoverwaltungssystem bei Abholung der zum Abschlusss der Geräteregistrierung benötigten Daten.

Secure Messaging Sitzungsschlüssel Sitzungs-Schlüssel der Secure Messaging Verbindung mit der eGK. Für die Kommunikation mit der eGK agiert der TOE als Terminal (Proximity Coupling Device, PCD) für die Ausführung des PACE-Protokolls [TR-03110-2]. Daher werden in den Sitzungsdaten auch die Secure Messaging Schlüssel vorgehalten.

TLS Sitzungsschlüssel Ephemerale Schlüssel der TLS Verbindung.

VAU-Protokoll Sitzungsschlüssel Ephemerale Schlüssel der VAU-Protokollsitzung.

X.509 Internet-Zertifikate für TLS-Verbindungen Öffentliche Zertifikate der TLS-Kommunikationspartner wie z.B. Zugangsgateway.

X.509 Zertifikate für Telematikinfrastruktur-Identitäten Öffentliche Zertifikate der Telematikinfrastruktur-Kommunikationspartner wie z.B. Dokumentenverwaltung.

Aktenschlüssel (RecordKey) entschlüsselter Aktenschlüssel

Kontextschlüssel (ContextKey) entschlüsselter Kontextschlüssel

6.2. Funktionale Sicherheitsanforderungen

6.2.1. Schutz von Geheimnissen

FPT_EMS.1
Emanation of TSF and User data

Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit sensitive data (as listed below) — or information which can be used to recover such sensitive data — through any interfaces[1] in excess of limits that ensure that no leakage of this sensitive data occurs[2] enabling access to TLS Sitzungsschlüssel, VAU-Protokoll Sitzungsschlüssel, SigD-Schlüsselpaar, Zustand des DRNG, Prüfcode, Aktenschlüssel (RecordKey), Kontextschlüssel (ContextKey), ECIES-Protokoll Sitzungsschlüssel, Secure Messaging Sitzungsschlüssel, RegistrationToken[3] and Aktenkonto, Berechtigungen, Gerätedaten, Gerätedaten Signaturdienst, Metadaten, PIN, AktenID (RecordIdentifier), Status Nutzer (Aktenkontoinhaber oder Vertreter), Liste der vergebenen Berechtigungen, Authentisierungstoken (AuthenticationAssertion), Autorisierungstoken (AuthorizationAssertion), Zustand des Aktenkontos (RecordState), Nutzerdaten, Konfigurationsdaten [4].
FPT_EMS.1.2	The TSF shall ensure Angreifer[5] are unable to use the following interface all interfaces[6] to gain access to TLS Sitzungsschlüssel, VAU-Protokoll Sitzungsschlüssel, SigD-Schlüsselpaar, Zustand des DRNG, Prüfcode, Aktenschlüssel (RecordKey), Kontextschlüssel (ContextKey), ECIES-Protokoll Sitzungsschlüssel, Secure Messaging Sitzungsschlüssel, RegistrationToken[7] and Aktenkonto, Berechtigungen, Gerätedaten, Gerätedaten Signaturdienst, Metadaten, PIN, AktenID (RecordIdentifier), Status Nutzer (Aktenkontoinhaber oder Vertreter), Liste der vergebenen Berechtigungen, Authentisierungstoken (AuthenticationAssertion), Autorisierungstoken (AuthorizationAssertion), Zustand des Aktenkontos (RecordState), Nutzerdaten, Konfigurationsdaten [8].

[1] Assignment: *types of emissions*
[2] Assignment: *specified limits*
[3] Assignment: *list of types of TSF data*
[4] Assignment: *list of types of user data*
[5] Assignment: *type of users*
[6] Assignment: *type of connection*
[7] Assignment: *list of types of TSF data*
[8] Assignment: *list of types of user data*

FDP_RIP.1
Subset residual information protection

Hierarchical to:	No other components
Dependencies:	No dependencies
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[9] the following objects: ECIES-Protokoll Sitzungsschlüssel, Secure Messaging Sitzungsschlüssel, TLS Sitzungsschlüssel, Aktenschlüssel (RecordKey), Kontextschlüssel (ContextKey), VAU-Protokoll Sitzungsschlüssel, PIN, Metadaten[10].
Refinement:	**These sensitive objects are overwritten with constant or pseudo-random values.**

6.2.2. Kryptographische Basisdienste

FCS_CKM.4
Cryptographic key destruction

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] hier erfüllt durch: FCS_CKM.1/Dok-Schlüssel, FCS_CKM.1/TLS, FCS_CKM.1/VAU, FCS_CKM.1/SM und FCS_CKM.1/PACE
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method by overwriting with zeros[11] that meets the following: none[12].
ST-Anwendungshinweis 1	FCS_CKM.4.1 zerstört die von den Komponenten FCS_COP.1/... benötigten Schlüssel. Gleiches gilt für die in Unterabschnitt 6.2.7 für TLS-Kanäle verwendeten Schlüssel. Die Schlüssel werden dabei mit Nullen überschrieben.
ST-Anwendungshinweis 2	Die Operationen entsprechen den Anforderungen in den Dokumenten [TR-03116-1] und [gemSpec_Krypt].

[9] Selection: *allocation of the resource to, deallocation of the resource from*
[10] Assignment: *list of objects*
[11] Assignment: *cryptographic key destruction method*
[12] Assignment: *list of standards*

FCS_COP.1/AES
Cryptographic operation / 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] hier erfüllt durch: FCS_CKM.1/Dok-Schlüssel FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/AES	The TSF shall perform symmetric encryption and decryption[13] in accordance with a specified cryptographic algorithm AES im GCM Modus mit Tag-Länge 128 Bit[14] and cryptographic key sizes 128 Bit und 256 Bit[15] that meet the following: FIPS 197 [FIPS PUB 197], RFC 3268 [RFC 3268], RFC 5289 [RFC 5289], NIST SP 800-38D [NIST SP 800-38D], specification [gemSpec_Krypt][16].

FCS_RNG.1
Generation of random numbers

Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RNG.1.1	The TSF shall provide a *deterministic*[17] random number generator that implements: (DRG.3.1) If initialized with a random seed using an NPTRNG of class NTG.1, the internal state of the RNG shall have an entropy of at least 200 bits. (DRG.3.2) The RNG provides forward secrecy. (DRG.3.3) The RNG provides backward secrecy even if the current internal state is known. [18]
FCS_RNG.1.2	The TSF shall provide random numbers that meet: (DRG.3.4) The RNG initialized with a random seed holding at least 200 bits of entropy generates output for which 2^{14} strings of bit length 128 are mutually different with probability $P > 1 - 2^{-8}$.

[13] Assignment: *list of cryptographic operations*
[14] Assignment: *cryptographic algorithm*
[15] Assignment: *cryptographic key sizes*
[16] Assignment: *list of standards*
[17] Selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*
[18] Assignment: *list of security capabilities*

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

[19]

ST-Anwendungshinweis 3 The deterministic random number generator used by OpenSSL is compliant to NIST SP800-90A [NIST SP 800-90A].

6.2.3. eGK-Kommunikation

Für die sichere Kommunikation mit der eGK über die kontaktlose-Schnittstelle werden vom TOE kryptographische Dienste bereitgestellt. Diese basieren auf elliptischen Kurven (ECC) definiert in RFC5639 [RFC 5639] mit den folgenden Parametern:

1. Länge 256 Bit: BrainpoolP256r1
2. Länge 384 Bit: BrainpoolP384r1
3. Länge 512 Bit: BrainpoolP512r1

Die zum Einsatz kommenden Authentisierungsprotokolle einigen sich auf gemeinsame Parameter um Authentizitätsschlüssel und, sofern Secure Messaging mit Verschlüsselung benötigt wird, Verschlüsselungsschlüssel für Secure Messaging zu erstellen.

FCS_COP.1/SM.SHA
Cryptographic operation

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.
FCS_COP.1.1/SM.SHA	The TSF shall perform hash value calculation[20] in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512[21] and cryptographic key sizes none[22] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4][23].

[19] Assignment: *a defined quality metric*
[20] Assignment: *list of cryptographic operations*
[21] Assignment: *cryptographic algorithm*
[22] Assignment: *cryptographic key sizes*
[23] Assignment: *list of standards*

FCS_COP.1/SM.AES
Cryptographic operation

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/SM FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/SM.AES	The TSF shall perform symmetric encryption and decryption for secure messaging and decryption and encryption for trusted channel (PACE)[24] in accordance with a specified cryptographic algorithm AES im CBC Modus[25] and cryptographic key sizes 128, 192, und 256 Bit[26] that meet the following: TR-03116 [TR-03116-1], FIPS 197 [FIPS PUB 197], NIST SP 800-38A [NIST SP 800-38A][27].

FCS_CKM.1/SM
Cryptographic key generation

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/SM.AES und FCS_COP.1/SM.CMAC FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.1.1/SM	The TSF shall generate cryptographic **session** keys in accordance with a specified cryptographic key generation algorithm $KDF_{Session}$ with the hash function SHA-1 to derive 128-bit AES keys and the hash function SHA-256 to derive 192-bit and 256-bit AES keys[28] and specified cryptographic key sizes 128 bit, 192 bit, und 256 bit[29] that meet the following: TR-03111 as specified in sec. 4.3.3.2 in [TR-03111] und FIPS 197 [FIPS PUB 197][30].

[24] Assignment: *list of cryptographic operations*
[25] Assignment: *cryptographic algorithm*
[26] Assignment: *cryptographic key sizes*
[27] Assignment: *list of standards*
[28] Assignment: *cryptographic key generation algorithm*
[29] Assignment: *cryptographic key sizes*
[30] Assignment: *list of standards*

FCS_CKM.1/PACE
Cryptographic key generation

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/SM.AES und FCS_COP.1/SM.CMAC FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.1.1/PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [TR-03111] using the protocol id-PACE-ECDH-GM-AES-CBC-CMAC-128 mit brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 mit brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 mit brainpoolP512r1[31] and specified cryptographic key sizes 256 bit, 384 bit, und 512 bit[32] that meet the following: TR-03110-2 [TR-03110-2] und TR-03111 [TR-03111][33].
ST-Anwendungshinweis 4	The TOE exchanges a shared secret with the external entity during the PACE protocol, see [TR-03110-2]. This protocol is based on the ECDH compliant to TR-03111 [TR-03111] (i.e. the elliptic curve cryptographic algorithm ECKA). The shared secret is used for deriving the AES session keys for message encryption and message authentication according to [TR-03110-2] for the TSF as required by, FCS_COP.1/SM.AES, and FCS_COP.1/SM.CMAC. FCS_CKM.1.1/PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to TR-03110 [TR-03110-2].

FCS_COP.1/SM.CMAC
Cryptographic operation

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

[31] Assignment: *cryptographic key generation algorithm*
[32] Assignment: *cryptographic key sizes*
[33] Assignment: *list of standards*

FCS_COP.1.1/SM.CMAC	The TSF shall perform computation and verification of cryptographic checksum for secure messaging[34] in accordance with a specified cryptographic algorithm AES-CMAC[35] and cryptographic key sizes 128, 192, und 256 Bit[36] that meet the following: NIST SP800-38B [NIST SP 800-38B], FIPS PUB 197 [FIPS PUB 197]. [37]

FTP_ITC.1/SM
Inter-TSF trusted channel / SM

Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_ITC.1.1/SM	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SM	The TSF shall permit *the TSF*[38] to initiate communication via the trusted channel.
FTP_ITC.1.3/SM	The TSF shall initiate communication via the trusted channel for Kommunikation mit der eGK[39].

6.2.4. Trust-Service Status List

FCS_COP.1/TSL.ECDSA
Cryptographic operation / ECDSA for TSL

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] not fulfilled in this ST as no keys have to be generated for signature verification. The public key for signature verification is available as part of the TOE and has been inserted during build time as part of the TI-Vertrauensanker. FCS_CKM.4 Cryptographic key destruction Cryptographic key destruction is not fulfilled in this ST as only public keys are used for this operation.

[34] Assignment: *list of cryptographic operations*
[35] Assignment: *cryptographic algorithm*
[36] Assignment: *cryptographic key sizes*
[37] Assignment: *list of standards*
[38] Selection: *the TSF, another trusted IT product*
[39] Assignment: *list of functions for which a trusted channel is required*

FCS_COP.1.1/TSL.ECDSA	The TSF shall perform verification of ECDSA signatures[40] in accordance with a specified cryptographic algorithm ecdsa-with-Sha256[41] and cryptographic key sizes 256 Bit[42] that meet the following: Spezifikation [gemSpec_Krypt], [TR-03116-1], [TR-03111]; [FIPS PUB 186-4][43].
ST-Anwendungshinweis 5	Der TOE verwendet ausschließlich die Kurve brainpoolP256r1 [RFC 5639; RFC 7027] für die Verifikation der Signaturen.
ST-Anwendungshinweis 6	Der TOE verwendet ausschließlich die nach ECC-Migration nutzbare TSL(ECC-RSA), vgl. [gemSpec_TSL, Kapitel 2.3] und [gemSpec_Krypt, Kapitel 5.3]. Daher ist die Beschränkung auf ECDSA ausreichend.

6.2.5. VAU-Protokoll

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 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*[44] 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 Kommunikation mit der Dokumentenverwaltung[45].
ST-Anwendungshinweis 7	Die redaktionellen Verfeinerungen am SFR-Text verdeutlichen die Forderung nach einer spezifikationskonformen Umsetzung des VAU-Protokolls durch den TOE.

[40] Assignment: *list of cryptographic operations*
[41] Assignment: *cryptographic algorithm*
[42] Assignment: *cryptographic key sizes*
[43] Assignment: *list of standards*
[44] Selection: *the TSF, another trusted IT product*
[45] Assignment: *list of functions for which a trusted channel is required*

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.
FCS_COP.1.1/VAU.HASH	The TSF shall perform hash value calculation[46] in accordance with a specified cryptographic algorithm SHA-1, SHA-256[47] and cryptographic key sizes none[48] that meet the following: FIPS 180-4 [FIPS PUB 180-4][49].
ST-Anwendungshinweis 8	Die Verwendung der unsicheren Hash-Funktion SHA-1 geht aus den Anforderungen an OCSP in [gemSpec_Krypt] A_17070-01 hervor.

FCS_CKM.1/VAU
Cryptographic key generation

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
FCS_CKM.1.1/VAU	The TSF shall generate cryptographic keys **for authenticated data encryption with AES-GCM-256** in accordance with a specified cryptographic key generation algorithm mutually authenticated ECDH based on brainpoolP256r1, and HKDF with SHA-256[50] and specified cryptographic key sizes 256 bit[51] that meet the following: VAU protocol [gemSpec_Krypt, Chapter 6] brainpoolP256r1 RFC 5639 [RFC 5639], ECC TR-03111 [TR-03111], ECDH NIST-800-56A [NIST SP 800-56-A], HKDF RFC 5869 [RFC 5869], SHA FIPS 180-4 [FIPS PUB 180-4]

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

[52].

ST-Anwendungshinweis 9 — Alle erzeugten Schlüssel müssen im Wesentlichen 256 Bit Entropie enthalten, da sie Teil eines hybriden Verfahrens sind in dem der symmetrische Anteil Schlüssel mir einer Länge von 256 Bit verwendet (siehe [[TR-03116-1], Abschnitt 3.9]).

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 10
FCS_CKM.4 Cryptographic key destruction
hier erfüllt durch: FCS_CKM.4

FCS_COP.1.1/VAU.ECDSA — The TSF shall perform peer authentication by verification of ECDSA signatures[53] in accordance with a specified cryptographic algorithm ECDSA in X.92 format with OID ecdsa-with-Sha256 with curve brainpoolP256r1[54] and cryptographic key sizes 256 bit[55] 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],
ECDSA format	TR-03111 [TR-03111, Chapter 5.2.2],
DSS	FIPS 186-4 [FIPS PUB 186-4],
SHA	FIPS PUB 180-4 [FIPS PUB 180-4]

[56].

ST-Anwendungshinweis 10 — Die *signature creation* wird von der eGK oder dem Signaturdienst durchgeführt und liegt somit in der Umgebung des TOE. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der eGK oder dem Signaturdienst. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* wird im TOE durchgeführt. Die Interpretation von VAU-Server-Zertifikaten wird durch FPT_TDC.1/VAU.Zert erbracht.

[52] Assignment: *list of standards*
[53] Assignment: *list of cryptographic operations*
[54] Assignment: *cryptographic algorithm*
[55] Assignment: *cryptographic key sizes*
[56] Assignment: *list of standards*

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

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_TDC.1.1/VAU.Zert	The TSF shall provide the capability to consistently interpret X.509 certificates of VAU server and the TSL[57] 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) (3) ob ein Zertifikat in einer gültigen Zertifikatskette bis zu einer zulässigen CA in der TSL enthalten ist, (4) Sperrstatus per OCSP-Anfrage [58] when interpreting the TSF data from ~~another trusted IT product~~ **VAU server endpoint**.
ST-Anwendungshinweis 11	Das hier verwendete OCSP-Protokoll basiert auf der unsicheren Hash-Funktion SHA-1, dies geht aus den Anforderungen an OCSP in [gemSpec_Krypt] A_17070-01 hervor.

FCS_COP.1/VAU.AES
Cryptographic operation/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] hier erfüllt durch: FCS_CKM.1/VAU FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/VAU.AES	The TSF shall perform authenticated symmetric encryption and decryption[59] in accordance with a specified cryptographic algorithm

[57] Assignment: *list of TSF data types*
[58] Assignment: *list of interpretation rules to be applied by the TSF*
[59] Assignment: *list of cryptographic operations*

	AES-GCM with tag length 128 bit[60] and cryptographic key sizes 256 bit[61] that meet the following: FIPS 197 [FIPS PUB 197], NIST SP 800-38D [NIST SP 800-38D][62].
ST-Anwendungshinweis 12	Der Initialisierungsvektor hat eine Länge von 96 Bit und wird aus dem sicheren Zufallsgenerator nach FCS_RNG.1 erzeugt.

6.2.6. Ver- und Entschlüsseln von Dokumenten

Das ePA Modul FdV unterstützt nur die symmetrische Verschlüsselung der Dokumente. Diese ist AES-basiert. Jedes Dokument wird mit dem zugehörigen Dokumentenschlüssel ver- bzw. entschlüsselt. Der Dokumentenschlüssel wird bei Dokumenten, die von der Dokumentenverwaltung bezogen werden, als mit dem Aktenschlüssel verschlüsseltes Chiffrat mit dem Dokument ausgeliefert. Beim Einstellen von neuen Dokumenten wird der Dokumentenschlüssel lokal erzeugt. Beim Aktivieren des Aktenkontos werden auch Akten- und Kontextschlüssel vom TOE erzeugt.

FCS_CKM.1/Dok-Schlüssel
Cryptographic key generation

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/AES FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.1.1/Dok-Schlüssel	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Direct Generation[63] and specified cryptographic key sizes 256 bit[64] that meet the following: NIST SP800-133 Kap. 6.1 [NIST SP 800-133 Rev. 2], TR-03116 [TR-03116-1] und [FIPS PUB 197][65].

6.2.7. TLS-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

Hierarchical to:	No other components
Dependencies:	No dependencies

[60] Assignment: *cryptographic algorithm*
[61] Assignment: *cryptographic key sizes*
[62] Assignment: *list of standards*
[63] Assignment: *cryptographic key generation algorithm*
[64] Assignment: *cryptographic key sizes*
[65] Assignment: *list of standards*

FTP_ITC.1.1/TLS	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification ~~or~~ **and** disclosure.
FTP_ITC.1.2/TLS	The TSF shall permit *the TSF*[66] to initiate communication via the trusted channel.
FTP_ITC.1.3/TLS	The TSF shall initiate communication via the trusted channel for Kommunikation mit dem Zugangsgateway, dem Signaturdienst und dem Kontoverwaltungssystem (siehe Tabelle B.4 für eine genaue Auflistung der einzelnen Verbindungen)[67].
ST-Anwendungshinweis 13	Der TOE unterstützt TLS Version 1.2 [RFC 5246] und Version 1.3 [RFC 8446] (s. [gemSpec_Krypt]) für die Kommunikation zum Zugangsgateway und TLS Version 1.2 für die Kommunikation zum Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).

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

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_TDC.1.1/TLS.Zert	The TSF shall provide the capability to consistently interpret X.509 Internet-Zertifikate für TLS-Verbindungen[68] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/TLS.Zert	The TSF shall use TLS-Cert interpretation rules[69] (1) die Gültigkeitsdauer eines Zertifikates (2) ob ein Zertifikat in einer gültigen Zertifikatskette bis zu einer zulässigen CA enthalten ist (3) per OCSP-Anfrage, ob das Zertifikat gesperrt wurde when interpreting the ~~**TSF data**~~ **TLS-Server-Certificates** from another trusted IT product.

TLS-Cert interpretation rules as defined in A_15887-01 in [gemSpec_Frontend_Vers]: Das ePA-Frontend des Versicherten MUSS für die Prüfung des internetseitigen Zertifikats des Zugangsgateways des Versicherten das Zertifikat auf ein CA-Zertifikat einer CA, die die „CA/-Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted

[66] Selection: *the TSF, another trusted IT product*
[67] Assignment: *list of functions for which a trusted channel is required*
[68] Assignment: *list of TSF data types*
[69] Assignment: *list of interpretation rules to be applied by the TSF*

Certificates“ (https://cabforum.org/baseline-requirements-documents/) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als „ungültig“ bewerten. Es MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als „ungültig“ bewerten.

FCS_CKM.1/TLS
Cryptographic key generation / TLS

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_COP.1/TLS.AES und FCS_COP.1/TLS.HMAC FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.1.1/TLS	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm allen in Tabelle B.1 Aufgeführten TLS-Cipher-Suites[70] and specified cryptographic key sizes 128 Bit für AES-128, 256 Bit für AES-256, 256 Bit für die HKDF mit SHA-256[71] that meet the following: Spezifikation [gemSpec_Krypt], NISTSP800-56A [NIST SP 800-56-A], [RFC 5869], [RFC 5289], [FIPS PUB 180-4], [FIPS PUB 197] [72]. **Es müssen alle Cipher-Suites in Tabelle B.1 unterstützt werden. Für die Aushandlung des Schlüssels mittels ECDH dürfen nur die Kurven-Parameter in Tabelle B.2 eingesetzt werden.**
ST-Anwendungshinweis 14	Der TOE verwendet ausschließlich die Kurven brainpoolP256r1 oder P-256, aus Tabelle B.2, für die TLS-Kommunikation mit Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).
ST-Anwendungshinweis 15	Der TOE unterstützt TLS Version 1.2 [RFC 5246] und Version 1.3 [RFC 8446] (s. [gemSpec_Krypt]). Der TOE unterstützt alle im SFR genannten cipher suites als Algorithmen für TLS. Die Schlüsselerzeugung basiert auf dem Elliptic-Curve-Diffie-Hellman-Keyexchange-Protocol mit RSA- oder ECDSA-Signaturen (ECDHE_RSA und ECDHE_ECDSA nach [RFC 4492]). Die Auswahloperation zur Schlüssellänge hängt von den gewählten Algorithmen ab. Die Schlüssel werden für die TLS-Kommunikation zwischen dem TOE und anderen Komponenten genutzt. Es werden jeweils getrennte Schlüssel für jede Verwendung und Verschlüsselung nach FCS_COP.1/TLS.AES und FCS_COP.1/TLS.HMAC berechnet.

[70] Assignment: *cryptographic key generation algorithm*
[71] Assignment: *cryptographic key sizes*
[72] Assignment: *list of standards*

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

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/TLS FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/TLS.HMAC	The TSF shall perform HMAC value generation and verification[73] in accordance with a specified cryptographic algorithm HMAC with SHA-256, SHA-384[74] and cryptographic key sizes 256 und 384 Bit[75] that meet the following: RFC 2104 [RFC 2104], FIPS PUB 180-4 [FIPS PUB 180-4] and [TR-03116-1][76]
ST-Anwendungshinweis 16	Der TOE verwendet ausschließlich HMAC auf Basis von SHA-256 mit der Schlüssellänge 256 Bit für die TLS-Kommunikation mit Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).

FCS_COP.1/TLS.AES
Cryptographic operation/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] hier erfüllt durch: FCS_CKM.1/TLS FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/TLS.AES	The TSF shall perform symmetric encryption and decryption[77] in accordance with a specified cryptographic algorithm AES im GCM Modus mit Tag-Länge 128 Bit[78] and cryptographic key sizes 128 Bit und 256 Bit[79] that meet the following: FIPS 197 [FIPS PUB 197], RFC 3268 [RFC 3268], RFC 5289 [RFC 5289], NIST SP 800-38D [NIST SP 800-38D], specification [gemSpec_Krypt][80].

[73] Assignment: *list of cryptographic operations*
[74] Assignment: *cryptographic algorithm*
[75] Assignment: *cryptographic key sizes*
[76] Assignment: *list of standards*
[77] Assignment: *list of cryptographic operations*
[78] Assignment: *cryptographic algorithm*
[79] Assignment: *cryptographic key sizes*
[80] Assignment: *list of standards*

ST-Anwendungshinweis 17	Der TOE verwendet ausschließlich AES-256 mit der Schlüssellänge 256 Bit für die TLS-Kommunikation mit Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).

FCS_COP.1/TLS.Hash
Cryptographic operation / Hash for TLS

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction Alle bisher für FCS_COP.1/TLS.Hash genannten Abhängigkeiten werden nicht erfüllt. Begründung: Bei einem Hash-Algorithmus handelt es sich um einen kryptographischen Algorithmus, der keine kryptographischen Schlüssel verwendet. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels und zu seiner Zerstörung erforderlich.
FCS_COP.1.1/TLS.Hash	The TSF shall perform hash value calculation[81] in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384[82] and cryptographic key sizes none[83] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4][84].
ST-Anwendungshinweis 18	Die Verwendung der unsicheren Hash-Funktion SHA-1 geht aus den Anforderungen an OCSP in [gemSpec_Krypt] GS-A_5131 hervor.
ST-Anwendungshinweis 19	Der TOE verwendet ausschließlich SHA-256 für die TLS-Kommunikation mit Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).

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

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: ST-Anwendungshinweis 20 FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4

[81] Assignment: *list of cryptographic operations*
[82] Assignment: *cryptographic algorithm*
[83] Assignment: *cryptographic key sizes*
[84] Assignment: *list of standards*

FCS_COP.1/TLS.Auth.RSA	The TSF shall perform verification of RSA signatures[85] in accordance with a specified cryptographic algorithm RSASSA-PKCS1-v1_5 and RSASSA-PSS[86] and cryptographic key sizes 2048 Bit[87] that meet the following: specification [gemSpec_Krypt], [TR-03116-1], RFC 8017 [RFC 8017], RFC 5246 [RFC 5246], RFC 8446 [RFC 8446][88].
ST-Anwendungshinweis 20	Eine *signature creation* wird vom TOE nicht durchgeführt. Eine Authentifizierung des TOEs am TLS-Server findet nicht im TLS Protokoll statt. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* wird im TOE durchgeführt. Der öffentliche Schlüssel wird dabei aus dem TLS-Server-Zertifikat importiert. Die Interpretation von TLS-Server-Zertifikaten wird durch FPT_TDC.1/TLS.Zert erbracht.

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

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: ST-Anwendungshinweis 22 FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/TLS.Auth.ECDSA	The TSF shall perform verification of ECDSA signatures[89] in accordance with a specified cryptographic algorithm ecdsa-with-Sha256[90] and cryptographic key sizes 256 Bit[91] that meet the following: Spezifikation [gemSpec_Krypt], [TR-03116-1], [TR-03111], [FIPS PUB 186-4], RFC 5246 [RFC 5246], RFC 8446 [RFC 8446][92].
ST-Anwendungshinweis 21	Der TOE verwendet ausschließlich die Kurven brainpoolP256r1 oder P-256 für die TLS-Kommunikation mit Signaturdienst und Kontoverwaltungssystem (s. [atosAuth1_V2]).

[85] Assignment: *list of cryptographic operations*
[86] Assignment: *cryptographic algorithm*
[87] Assignment: *cryptographic key sizes*
[88] Assignment: *list of standards*
[89] Assignment: *list of cryptographic operations*
[90] Assignment: *cryptographic algorithm*
[91] Assignment: *cryptographic key sizes*
[92] Assignment: *list of standards*

ST-Anwendungshinweis 22 — Eine *signature creation* wird vom TOE nicht durchgeführt. Eine Authentifizierung des TOEs am TLS-Server findet nicht im TLS Protokoll statt. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* wird im TOE durchgeführt. Der öffentliche Schlüssel wird dabei aus dem TLS-Server-Zertifikat importiert. Die Interpretation von TLS-Server-Zertifikaten wird durch FPT_TDC.1/TLS.Zert erbracht.

6.2.8. Kryptographische Operationen zur Autorisierung mittels 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, das aus Akten- und Kontextschlüssel besteht, muss der TOE mit SGD1 und SGD2 sicher kommunizieren.

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**~~ **Schlüsselgenerierungsdienst** 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*[93] 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 1 und SGD 2[94].
ST-Anwendungshinweis 23	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 Abschnitt 7.6.1 hergestellt.

[93] Selection: *the TSF, another trusted IT product*
[94] Assignment: *list of functions for which a trusted channel is required*

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] 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[95] in accordance with a specified cryptographic algorithm SHA-1, SHA-256[96] and cryptographic key sizes none[97] that meet the following: FIPS 180-4 [FIPS PUB 180-4][98].
ST-Anwendungshinweis 24	Die Verwendung der unsicheren Hash-Funktion SHA-1 geht aus den Anforderungen an OCSP in [gemSpec_Krypt] A_17070-01 hervor.

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[99] 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.

[95] Assignment: *list of cryptographic operations*
[96] Assignment: *cryptographic algorithm*
[97] Assignment: *cryptographic key sizes*
[98] Assignment: *list of standards*
[99] Assignment: *access control SFP(s) and/or information flow control SFP(s)*

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 by *getPublicKey* operation[100].

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[101] on subject Nutzer, object public ECIES key of SGD, operation import[102].

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 25
FDP_ACF.1.1/SGD	The TSF shall enforce the SGD public key import SFP[103] to objects based on the following: subject Nutzer, object public ECIES key of SGD with security attributes ECDSA signature and certificate, operation import[104].
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 Nutzer may import object public ECIES key of SGD 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

[100] Assignment: *additional importation control rules*
[101] Assignment: *access control SFP*
[102] Assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*
[103] Assignment: *access control SFP*
[104] 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*

[105].

FDP_ACF.1.3/SGD	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[106].
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 may not be imported by Nutzer except for accessing SGD with SGD protocol[107].
ST-Anwendungshinweis 25	Die Abhängigkeit zu FMT_MSA.3 nicht erfüllt: Für das Datenobjekt „public ECIES key of SGD“ 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
FCS_COP.1.1/SGD.ECDSA	The TSF shall perform data authentication by verification of ECDSA signatures[108] in accordance with a specified cryptographic algorithm ECDSA in X.92 format with OID ecdsa-with-Sha256 with curve brainpoolP256r1[109] and cryptographic key sizes 256 bit[110] that meet the following:

SGD protocol	gematik spec. [gemSpec_SGD_ePA, Chapter 2.3],
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 186-4 [FIPS PUB 186-4],
SHA	FIPS 180-4 [FIPS PUB 180-4]

[111].

[105] Assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*
[106] Assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*
[107] Assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*
[108] Assignment: *list of cryptographic operations*
[109] Assignment: *cryptographic algorithm*
[110] Assignment: *cryptographic key sizes*
[111] Assignment: *list of standards*

ST-Anwendungshinweis 26 — Die *signature creation* wird von der eGK oder dem Signaturdienst durchgeführt und liegt somit in der Umgebung des TOE. Der verwendete private Schlüssel verbleibt dabei immer innerhalb der eGK oder dem Signaturdienst. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels erforderlich. Die *verification of digital signatures* wird im TOE durchgeführt. Die Interpretation von SGD-Server-Zertifikaten wird durch FPT_TDC.1/SGD.Zert erbracht.

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 and the TSL[112] 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 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`, (3) ob ein Zertifikat einer gültigen Zertifikatskette bis zu einer zulässigen CA in der TSL enthalten ist [113] when interpreting the TSF data from ~~**another trusted IT product**~~ **Schlüsselgenerierungsdienst**.

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

[112] Assignment: *list of TSF data types*
[113] Assignment: *list of interpretation rules to be applied by the TSF*

FCS_COP.1.1/SGD.ECIES

The TSF shall perform ECIES-based authenticated hybrid encryption and decryption[114] 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[115] and cryptographic key sizes 256 bit[116] that meet the following:

ECIES	[SEC1-2009],
brainpoolP256r1	RFC 5639 [RFC 5639],
ECC	TR-03111 [TR-03111],
ECDH	NIST-800-56A [NIST SP 800-56-A],
HKDF	RFC 5869 [RFC 5869],
SHA	FIPS 180-4 [FIPS PUB 180-4],
AES	FIPS 197 [FIPS PUB 197],
GCM	NIST SP 800-38D [NIST SP 800-38D]

[117].

ST-Anwendungshinweis 27

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 Abschnitt 7.6 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.

ST-Anwendungshinweis 28

Der Initialisierungsvektor für AES-GCM hat eine Länge von 96 Bit und wird aus dem sicheren Zufallsgenerator nach FCS_RNG.1 erzeugt.

6.2.9. Kryptographische Operationen zur Autorisierung des Kontoverwaltungssystems

Die Registrierung eines Gerät des Versicherten und ggf. die Anlage einer al.vi erfolgt über das OAuth 2.0 Protokoll mit der Proof Key for Code Exchange (PKCE) Erweiterung. Dabei autorisiert der Nutzer das Kontoverwaltungssystem am Signaturdienst das Gerät des Versicherten zu registrieren und dafür – falls notwendig – eine al.vi anzulegen und die dazu benötigten Daten zu übertragen. Für die Authentifizierung gegenüber dem Kontoverwaltungssystem wird ein temporäres Geheimnis, der Prüfcode vom TOE erzeugt. Mit diesem Prüfcode wird sicherstellt, dass nur das den Prozess anstoßende Gerät des Versicherten die am Ende des Prozesses durch das Kontoverwaltungssystem bereitgestellten Daten abrufen kann. Im Zuge des Prozesses wird durch das Kontoverwaltungssystem eine Geräte ID erzeugt.

[114] Assignment: *list of cryptographic operations*
[115] Assignment: *cryptographic algorithm*
[116] Assignment: *cryptographic key sizes*
[117] Assignment: *list of standards*

FCS_COP.1/OAUTH.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] FCS_CKM.4 Cryptographic key destruction Alle bisher für FCS_COP.1/OAUTH.HASH genannten Abhängigkeiten werden nicht erfüllt. Begründung: Bei einem Hash-Algorithmus handelt es sich um einen kryptographischen Algorithmus, der keine kryptographischen Schlüssel verwendet. Daher ist auch keine Funktionalität zum Import bzw. zur Generierung des kryptographischen Schlüssels und zu seiner Zerstörung erforderlich.
FCS_COP.1.1/OAUTH.HASH	The TSF shall perform hash value calculation[118] in accordance with a specified cryptographic algorithm SHA-256[119] and cryptographic key sizes none[120] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4], [RFC 7636][121].

6.2.10. Kryptographische Operationen zur Authentifizierung gegenüber dem Signaturdienst

Die Authentifizierung der Nachrichten des TOE gegenüber dem Signaturdienst wird mit JSON Web Signatures (JWS) durchgeführt. Hierfür wird ein dediziertes Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel erzeugt. Der öffentliche Schlüssel wird dem Signaturdienst zur Verfügung gestellt. Der zugehörige private Schlüssel verbleibt auf dem Gerät des Versicherten und wird dort sicher abgelegt. Dieser wird anschließend verwendet, um die Nachrichten an den Signaturdienst zu signieren.

FTP_ITC.1/JWS
Inter-TSF trusted channel / JWS

Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_ITC.1.1/JWS	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[118] Assignment: *list of cryptographic operations*
[119] Assignment: *cryptographic algorithm*
[120] Assignment: *cryptographic key sizes*
[121] Assignment: *list of standards*

FTP_ITC.1.2/JWS	The TSF shall permit *the TSF*[122] to initiate communication via the trusted channel.
FTP_ITC.1.3/JWS	The TSF shall initiate communication via the trusted channel for Kommunikation mit dem Signaturdienst[123].

FCS_COP.1/JWS.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: FCS_CKM.1/JWS.KEYS FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_COP.1.1/JWS.ECDSA	The TSF shall perform creating of ECDSA signatures[124] in accordance with a specified cryptographic algorithm ecdsa-with-Sha256[125] and cryptographic key sizes 256 Bit[126] that meet the following: Spezifikation [RFC 7515], [TR-03116-1], [TR-03111]; [FIPS PUB 186-4][127].

FCS_CKM.1/JWS.KEYS
Cryptographic key generation / ECDSA

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] hier erfüllt durch: FCS_CKM.2/JWS.ECDSA FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.1.1/JWS.KEYS	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Key Pair Generation by Testing Candidates[128] and specified cryptographic key sizes 256 Bit[129] that meet the following: Kurven-Parameter brainpoolP256r1

[122] Selection: *the TSF, another trusted IT product*
[123] Assignment: *list of functions for which a trusted channel is required*
[124] Assignment: *list of cryptographic operations*
[125] Assignment: *cryptographic algorithm*
[126] Assignment: *cryptographic key sizes*
[127] Assignment: *list of standards*
[128] Assignment: *cryptographic key generation algorithm*
[129] Assignment: *cryptographic key sizes*

[RFC 5639], NIST P-256 [FIPS PUB 186-4], NIST SP800-56A Kapitel 5.6.1.2.2 [NIST SP 800-56-A], TR-03116 [TR-03116-1][130].

Für die Erzeugung eines Schlüssels für das ECDSA-Verfahren müssen nach [atosAuth1_V2] die Kurven-Parameter brainpoolP256r1 [RFC 5639] oder NIST P-256 [FIPS PUB 186-4] verwendet werden.

Die Implementierung der Schlüsselgenerierung (Key Pair Generation by Testing Candidates) weicht vom NIST Standard (NIST SP800-56A Kapitel 5.6.1.2.2 [NIST SP 800-56-A]) ab.

FCS_CKM.2/JWS.ECDSA
Cryptographic key distribution / ECDSA

Einmalige Übermittlung des öffentlichen Schlüssels für die JWS.

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/JWS.KEYS FCS_CKM.4 Cryptographic key destruction hier erfüllt durch: FCS_CKM.4
FCS_CKM.2.1/JWS.ECDSA	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ephemerer ECDH auf basis der Kurven brainpoolP256r1 oder P-256[131] that meets the following standard: [RFC 5639], [NIST SP 800-56-A], [TR-03116-1] and [FIPS PUB 186-4][132].

6.3. Sicherheitsanforderungen an die Vertrauenswürdigkeit des TOE

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit für dieses Security Target ergeben sich aus den Anforderungen in [gemSpec_Frontend_Vers].

Die wesentlichen Punkte sind das Verbot die Sessiondaten, Schlüsselmaterial und die Authentisierungsmerkmale (mit Ausnahme der Schlüssel zur Authentifizierung gegenüber dem Signaturdienst [atosAuth1_V2]) persistent zu speichern.

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit entsprechen EAL 2.

[130] Assignment: *list of standards*
[131] Assignment: *cryptographic key distribution method*
[132] Assignment: *list of standards*

6.4. Erklärung der Sicherheitsanforderungen

6.4.1. Erklärung der Abhängigkeiten der SFR

Die Abhängigkeiten der in Abschnitt 6.2 aufgestellten funktionalen Sicherheitsanforderungen sind bis auf einige Ausnahmen erfüllt. Dort, wo von einer Erfüllung abgesehen wurde, wird dies direkt erläutert.

Die Abhängigkeiten der Sicherheitsanforderungen sind bei der Definition des jeweiligen SFR notiert. Sie werden hier zur Übersicht tabellarisch wiederholt.

Die in Abschnitt 5.1 neu eingeführten Komponenten FCS_RNG.1 und FPT_EMS.1 haben keine Abhängigkeiten, die aufgelöst werden müssen.

Zur besseren Übersicht sind die folgenden Tabellen nach Sicherheitsfunktionalität geordnet.

Selbstschutz (SF.SelfProtection)

SFR	Abhängig von	Erfüllt durch
FDP_RIP.1	Keine Abhängigkeiten	-
FPT_EMS.1	Keine Abhängigkeiten	-

Kryptografische Dienste (SF.CryptographicServices)

SFR	Abhängig von	Erfüllt durch
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/Dok-Schlüssel, FCS_CKM.1/TLS, FCS_CKM.1/VAU, FCS_CKM.1/SM und FCS_CKM.1/PACE
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/Dok-Schlüssel, und FCS_CKM.4
FCS_RNG.1	Keine Abhängigkeiten	-
FCS_CKM.1/Dok-Schlüssel	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 FCS_COP.1/AES

TLS-Service (SF.TLS)

SFR	Abhängig von	Erfüllt durch
FTP_ITC.1/TLS	Keine Abhängigkeiten	-
FPT_TDC.1/TLS.Zert	Keine Abhängigkeiten	-
FCS_CKM.1/TLS	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/TLS.AES FCS_COP.1/TLS.HMAC FCS_CKM.4
FCS_COP.1/TLS.Auth.RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. ST-Anwendungshinweis 20 FCS_CKM.4
FCS_COP.1/TLS.Auth.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. ST-Anwendungshinweis 22 FCS_CKM.4
FCS_COP.1/TLS.AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/TLS, und FCS_CKM.4
FCS_COP.1/TLS.HMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/TLS FCS_CKM.4
FCS_COP.1/TLS.Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Keine der Abhängigkeiten werden erfüllt. (Begründung siehe FCS_COP.1/TLS.Hash)

VAU-Server-Protokoll (SF.VAU-Server-Protokoll)

SFR	Abhängig von	Erfüllt durch
FCS_CKM.1/VAU	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/VAU.AES FCS_CKM.4
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
FCS_COP.1/TSL.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. Def. FCS_COP.1/TSL.ECDSA
FCS_COP.1/VAU.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	s. ST-Anwendungshinweis 10 FCS_CKM.4
FPT_TDC.1/VAU.Zert	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	Keine der Abhängigkeiten werden erfüllt. (Begründung siehe FCS_COP.1/VAU.HASH)

SGD-Protokoll / ECIES-Verfahren (SF.SGD)

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
FCS_COP.1/SGD.Hash	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Keine Abhängigkeiten werden erfüllt da es keinen Schlüssel gibt
FTP_ITC.1/SGD	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
FPT_TDC.1/SGD.Zert	Keine Abhängigkeiten	-
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 25

eGK Kommunikation (SF.EGK)

SFR	Abhängig von	Erfüllt durch
FCS_CKM.1/SM	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 FCS_COP.1/SM.AES FCS_COP.1/SM.CMAC
FCS_CKM.1/PACE	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 FCS_COP.1/SM.AES FCS_COP.1/SM.CMAC
FCS_COP.1/SM.AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/SM FCS_CKM.4
FCS_COP.1/SM.CMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/SM FCS_CKM.4
FCS_COP.1/SM.SHA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Keine Abhängigkeiten werden erfüllt da es keinen Schlüssel gibt
FTP_ITC.1/SM	Keine Abhängigkeiten	-

SIGD Kommunikation (SF.SIGD)

SFR	Abhängig von	Erfüllt durch
FTP_ITC.1/JWS	Keine Abhängigkeiten	-
FCS_CKM.1/JWS.KEYS	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.4 FCS_CKM.2/JWS.ECDSA
FCS_CKM.2/JWS.ECDSA	[FDP_ITC.1 or FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.4 FCS_CKM.1/JWS.KEYS
FCS_COP.1/JWS.ECDSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.4 FCS_CKM.1/JWS.KEYS
FCS_COP.1/OAUTH.HASH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Keine der Abhängigkeiten werden erfüllt. (Begründung siehe FCS_COP.1/OAUTH.HASH)

6.4.2. Überblick der Abdeckung von Sicherheitszielen

Die Zuordnung von Sicherheitszielen zu Sicherheitsanforderungen ist in Tabelle 6.8 gezeigt.

	O.Basis.Krypto	O.eGK.SM	O.ECIES	O.VAU	O.Secure.Storage	O.Dok.Verschl	O.TLS.Krypto	O.OAUTH	O.Schutz.Mem	O.RNG	O.JWS
FCS_CKM.1/Dok-Schlüssel	✓	.	.	.	.	✓	.	.	.	.	.
FCS_CKM.1/SM	.	✓	.	.	.	.	.	.	.	.	.
FCS_CKM.1/PACE	.	✓	.	.	.	.	.	.	.	.	.
FCS_CKM.1/TLS	✓	.	.	.	.	.	✓	.	.	.	.
FCS_CKM.1/VAU	✓	.	.	✓	.	.	.	.	.	.	.
FCS_CKM.1/JWS.KEYS	✓	.	.	.	.	.	.	.	.	.	✓
FCS_CKM.2/JWS.ECDSA	✓	.	.	.	.	.	.	.	.	.	✓
FCS_CKM.4	✓	.	.	.	.	.	.	.	✓	.	.
FCS_COP.1/AES	✓	.	.	.	.	✓	.	.	.	.	.
FCS_COP.1/JWS.ECDSA	✓	.	.	.	.	.	.	.	.	.	✓
FCS_COP.1/OAUTH.HASH	✓	.	.	.	.	.	.	✓	.	.	.
FCS_COP.1/SGD.ECDSA	✓	.	✓	.	.	.	.	.	.	.	.
FCS_COP.1/SGD.Hash	✓	.	✓	.	.	.	.	.	.	.	.
FCS_COP.1/SGD.ECIES	✓	.	✓	.	.	.	.	.	.	.	.
FCS_COP.1/SM.AES	✓	✓	.	.	.	.	.	.	.	.	.
FCS_COP.1/SM.CMAC	✓	✓	.	.	.	.	.	.	.	.	.
FCS_COP.1/SM.SHA	✓	✓	.	.	.	.	.	.	.	.	.
FCS_COP.1/TLS.AES	✓	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/TLS.Auth.ECDSA	✓	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/TLS.Auth.RSA	✓	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/TLS.Hash	✓	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/TLS.HMAC	✓	.	.	.	.	.	✓	.	.	.	.
FCS_COP.1/TSL.ECDSA	✓	.	✓	✓	.	.	.	.	.	.	.
FCS_COP.1/VAU.AES	✓	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/VAU.ECDSA	✓	.	.	✓	.	.	.	.	.	.	.
FCS_COP.1/VAU.HASH	✓	.	.	✓	.	.	.	.	.	.	.
FCS_RNG.1	✓	.	.	.	.	.	.	.	.	✓	.
FDP_ACC.1/SGD	.	.	✓	.	.	.	.	.	.	.	.
FDP_ACF.1/SGD	.	.	✓	.	.	.	.	.	.	.	.
FDP_ITC.2/SGD	.	.	✓	.	.	.	.	.	.	.	.
FDP_RIP.1	.	.	.	.	.	.	.	.	✓	.	.
FPT_EMS.1	.	.	.	.	✓	.	.	.	✓	.	.
FPT_TDC.1/TLS.Zert	.	.	.	.	.	.	✓	.	.	.	.
FPT_TDC.1/SGD.Zert	.	.	✓	.	.	.	.	.	.	.	.
FPT_TDC.1/VAU.Zert	.	.	.	✓	.	.	.	.	.	.	.
FTP_ITC.1/SGD	.	.	✓	.	.	.	.	.	.	.	.
FTP_ITC.1/SM	.	✓	.	.	.	.	.	.	.	.	.
FTP_ITC.1/TLS	✓	.	.	.	.	.	✓	.	.	.	.
FTP_ITC.1/VAU	.	.	.	✓	.	.	.	.	.	.	.

Abbildung der Sicherheitsziele auf Sicherheitsanforderungen

	O.Basis.Krypto	O.eGK.SM	O.ECIES	O.VAU	O.Secure.Storage	O.Dok.Verschl	O.TLS.Krypto	O.OAUTH	O.Schutz.Mem	O.RNG	O.JWS
FTP_ITC.1/JWS	✓	.	.	.	.	.	.	.	.	.	✓

Tabelle 6.8.: Abbildung der Sicherheitsziele auf Sicherheitsanforderungen

6.4.3. Detaillierte Erklärung für die Sicherheitsziele

O.TLS.Krypto

Aspekt des Ziels	SFR
TLS-Kanäle	FPT_TDC.1/TLS.Zert FTP_ITC.1/TLS
	In O.TLS.Krypto wird gefordert: „Der TOE setzt TLS-Kanäle zur Gewährleistung der Integrität, Authentizität und Vertraulichkeit der Kommunikation mit anderen IT-Produkten ein.“ Genau dies leistet FTP_ITC.1/TLS. Zertifikate, die im Rahmen von TLS-Verbindungen zum Einsatz kommen, werden nach den Vorgaben in FPT_TDC.1/TLS.Zert interpretiert.
sichere kryptographische Algorithmen und Protokolle	FCS_COP.1/TLS.Auth.RSA FCS_COP.1/TLS.Auth.ECDSA FCS_CKM.1/TLS FCS_COP.1/TLS.HMAC FCS_COP.1/TLS.AES FCS_COP.1/TLS.Hash
	Für die TLS-Kanäle sind nach O.TLS.Krypto nur „sichere kryptographische Algorithmen und Protokolle gemäß [TR-03116-1] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [gemSpec_Krypt]“ zugelassen. FCS_COP.1/TLS.Auth.RSA und FCS_COP.1/TLS.Auth.ECDSA spezifizieren die für die Authentisierung im Rahmen des TLS- Verbindungsaufbaus eingesetzten Algorithmen. Welches der beiden Verfahren verwendet wird ist abhängig von der für die Verbindung eingesetzten CipherSuite. Auf Basis des ECDHE-Schlüsseleinigungsverfahrens wird ein gemeinsames Geheimnis zwischen Server und Client berechnet, das in FCS_CKM.1/TLS verwendet wird, um mittels einer HMAC (FCS_COP.1/TLS.HMAC) basierenden KDF Schlüssel für die symmetrische Verschlüsselung zwischen Server und Client mittel AES-256/GCM (FCS_COP.1/TLS.AES) zu erzeugen. Die Vertraulichkeit, Integrität und Authentizität der ausgetauschten Nachrichten wird nach dem initialen Verbindungsaufbau durch AES im GCM Modus gesichert (FCS_COP.1/TLS.AES, FCS_COP.1/TLS.Hash).

O.eGK.SM

Aspekt des Ziels	SFR
Kryptographische Absicherung (SM)	FCS_COP.1/SM.AES FCS_CKM.1/SM FCS_COP.1/SM.CMAC FTP_ITC.1/SM FCS_CKM.1/PACE FCS_COP.1.1/SM.SHA

In O.eGK.SM wird gefordert: „Der TOE setzt zur Gewährleistung der Integrität und Vertraulichkeit der Kommunikation mit der eGK Secure Messaging ein.“. Dazu kommen FCS_COP.1/SM.AES FCS_CKM.1/SM FCS_COP.1/SM.CMAC FTP_ITC.1/SM zum Einsatz. FCS_CKM.1/SM erfordert, dass die TSF bestimmte kryptographische Schlüssel (AES) mit bestimmten Schlüssellängen nach einer Vorschrift generiert. Dabei kommt auch FCS_COP.1.1/SM.SHA zum Einsatz. FCS_CKM.1/SM erfordert, dass die Erstellung der Sitzungsschlüssel mittels des PACE Protokolles nach Vorschriften generiert werden. FCS_COP.1/SM.AES erfordert, dass die TSF Ver- und Entschlüsselung mit AES mit unterschiedlichen Schlüssellängen für Secure Messaging bereitstellt. FCS_COP.1/SM.CMAC erfordert, dass die TSF die Berechnung und Verifikation von kryptographischen Checksummen mittels des auf AES basierenden CMAC Algorithmus mit unterschiedlichen Schlüssellängen für Secure Messaging bereitstellt. FTP_ITC.1/SM erfordert, dass die TSF einen Kommunikationskanal zwischen sich selbst und einem anderen vertrauenswürdigen IT-Produkt (eGK) bereitstellt. Der Kommunikationskanal liefert Identitätsgarantien der Endpunkte und Schutz der Daten im Bezug auf Vertraulichkeit und Integrität.

O.Secure.Storage

Aspekt des Ziels	SFR
Vertrauliche Speicherung von Daten	FPT_EMS.1

Das Sicherheitsziel O.Secure.Storage fordert „Der TOE speichert automatisch nur dann schützenswerte Daten und Konfigurationsparameter persistent, wenn dies für die Funktionsfähigkeit des ePA Modul FdV gemäß Spezifikation notwendig ist. In diesem Fall nutzt er zur Ablage von schützenswürdigen Daten und Konfigurationsparametern entweder direkt den vom Gerät des Versicherten zur Verfügung gestellten sicheren Speicher oder verschlüsselt die Daten mit kryptographischen Algorithmen gemäß Vorgaben und legt den Schlüssel in diesen sicheren Speicher ab.“ FPT_EMS.1

O.Basis.Krypto

Aspekt des Ziels	SFR
Basis Anforderungen an alle verwendeten kryptografische Operationen	FCS_CKM.1/Dok-Schlüssel FCS_CKM.1/TLS FCS_CKM.1/VAU FCS_CKM.1/JWS.KEYS FCS_CKM.2/JWS.ECDSA FCS_CKM.4 FCS_COP.1/AES FCS_COP.1/JWS.ECDSA FCS_COP.1/OAUTH.HASH FCS_COP.1/SGD.ECDSA FCS_COP.1/SGD.Hash FCS_COP.1/SGD.ECIES FCS_COP.1/SM.AES FCS_COP.1/SM.CMAC FCS_COP.1/SM.SHA FCS_COP.1/TLS.AES FCS_COP.1/TLS.Auth.ECDSA FCS_COP.1/TLS.Auth.RSA FCS_COP.1/TLS.Hash FCS_COP.1/TLS.HMAC FCS_COP.1/TSL.ECDSA FCS_COP.1/VAU.AES FCS_COP.1/VAU.ECDSA FCS_COP.1/VAU.HASH FCS_RNG.1 FTP_ITC.1/TLS FTP_ITC.1/JWS

Das Sicherheitsziel O.Basis.Krypto fordert die Verwendung von sicheren „kryptographische Algorithmen und Protokolle für alle Kryptoverfahren gemäß [TR-03116-1] mit den Einschränkungen der gematik Spezifikation für Kryptoalgorithmen [gemSpec_Krypt]“ für den TOE.
Alle vom TOE eingesetzten Verfahren erfüllen diese Anforderungen. Zufall wird nach den Anforderungen aus FCS_RNG.1 bezogen. Sämtliche generierte Schlüssel werden nach den Vorgaben aus FCS_CKM.4 wieder gelöscht. Schlüssel werden nach FCS_CKM.1/Dok-Schlüssel, FCS_CKM.1/TLS, FCS_CKM.1/VAU oder FCS_CKM.1/JWS.KEYS erzeugt. Dabei kommt auch FCS_COP.1/SM.SHA zum Einsatz. Verteilt werden Schlüssel mittels FCS_CKM.2/JWS.ECDSA. Für die symmetrische Verschlüsselung werden FCS_COP.1/AES. FCS_COP.1/TLS.AES, FCS_COP.1/SM.AES und FCS_COP.1/VAU.AES verwendet, für die Authentifizierung werden FCS_COP.1/SGD.ECDSA, FCS_COP.1/TLS.Auth.ECDSA, FCS_COP.1/TLS.Auth.RSA, FCS_COP.1/TLS.HMAC, FCS_COP.1/TSL.ECDSA, FCS_COP.1/VAU.ECDSA, FCS_COP.1/JWS.ECDSA verwendet. Daneben wird auch FCS_COP.1/SGD.ECIES eingesetzt. Um die Integrität von Daten festzustellen werden die Hash-Funktionen FCS_COP.1/SGD.Hash, FCS_COP.1/TLS.Hash, FCS_COP.1/VAU.HASH oder FCS_COP.1/OAUTH.HASH verwendet. Als sicherer Kanal wird TLS FTP_ITC.1/TLS eingesetzt und FTP_ITC.1/JWS.

O.RNG

Aspekt des Ziels	SFR
Zufallszahlengenerator	FCS_RNG.1
	In O.RNG wird gefordert: „Der TOE verwendet einen Zufallszahlengenerator, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klasse DRG.3 liefert.“ Genau dies leistet FCS_RNG.1

O.Schutz.Mem

Aspekt des Ziels	SFR
Speicheraufbereitung: temporäre Kopien nicht mehr benötigter Geheimnisse werden unmittelbar nach Gebrauch aktiv überschrieben	FDP_RIP.1 FCS_CKM.4
	In O.Schutz.Mem wird gefordert: „Der TOE löscht temporäre Kopien nicht mehr benötigter Geheimnisse (z. B. Schlüssel) vollständig durch aktives Überschreiben. Das Überschreiben erfolgt unmittelbar zu dem Zeitpunkt, an dem die Geheimnisse nicht mehr benötigt werden.“ Genau dies leistet FDP_RIP.1. Auch die Zuweisung „upon the deallocation of the resource from“ passt zur Forderung in O.Schutz.Mem. Die „Geheimnisse (z. B. Schlüssel)“ werden im SFR durch die Zuweisung präzisiert. Sämtliche generierte Schlüssel werden nach den Vorgaben aus FCS_CKM.4 wieder gelöscht.
Schutz gegen unbefugte Kenntnisnahme	FPT_EMS.1
	„Der TOE schützt sich selbst und die ihm anvertrauten Daten.“ Um den Aspekt „die ihm anvertrauten Daten“ vollständig abzudecken, wurde die explizite Komponente FPT_EMS.1 ergänzt. Dieses SFR fordert genau die Analyse, ob andere Möglichkeiten zur unbefugten Kenntnisnahme bestehen.

O.VAU

Aspekt des Ziels	SFR
VAU-Kanäle	FTP_ITC.1/VAU FPT_TDC.1/VAU.Zert
	In O.VAU wird gefordert: „Der TOE setzt das VAU-Protokoll zur Gewährleistung der Integrität und Vertraulichkeit während der Kommunikation mit der Dokumentenverwaltung ein.“ Genau dies leistet FTP_ITC.1/VAU. Zertifikate, die im Rahmen von VAU-Verbindungen zum Einsatz kommen, werden nach den Vorgaben in FPT_TDC.1/VAU.Zert interpretiert.
VAU-Protokoll zur sicheren Kommunikation mit der Dokumentenverwaltung	FCS_COP.1/TSL.ECDSA FCS_COP.1/VAU.ECDSA FCS_COP.1/VAU.AES FCS_COP.1/VAU.HASH FCS_CKM.1/VAU FPT_TDC.1/VAU.Zert
	In O.VAU wird gefordert, dass die Anforderungen aus Kapitel 6 der Übergreifenden Spezifikation: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur [gemSpec_Krypt] für das VAU-Protokoll umgesetzt werden. Die Erzeugung von Schlüsseln wird in FCS_CKM.1/VAU gefordert. Die zu übertragenen Daten werden nach FCS_COP.1/VAU.ECDSA authentifiziert, hierzu muss der öffentliche Schlüssel des Servers importiert werden (FPT_TDC.1/VAU.Zert). Dies erfordert gleichzeitig die Authentisierung und Verifikation der Zertifikate nach FCS_COP.1/TSL.ECDSA. Der eigentliche Schutz der Daten wird erfüllt durch die Verschlüsselungsfunktion, kompatibel zu den Anforderungen in FCS_COP.1/VAU.AES. Die Hashfunktion mit den Anforderungen FCS_COP.1/VAU.HASH gewährleistet die geforderte Integrität für das Protokoll.

Aspekt „Sicherer Kanal zum VAU-Server-Endpunkt“

In O.VAU 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. Die Schlüsselvernichtung übernimmt FCS_CKM.4.

O.ECIES

Aspekt des Ziels	SFR
ECIES-Kanäle	FTP_ITC.1/SGD FPT_TDC.1/SGD.Zert In O.ECIES wird gefordert: „Der TOE setzt das ECIES-Protokoll zur Gewährleistung der Integrität und Vertraulichkeit während der Kommunikation mit den Schlüsselgenerierungsdiensten ein.“ Genau dies leistet FTP_ITC.1/SGD. Zertifikate, die im Rahmen von ECIES-Verbindungen zum Einsatz kommen, werden nach den Vorgaben in FPT_TDC.1/SGD.Zert interpretiert.
ECIES-Protokoll zur sicheren Kommunikation mit dem Schlüsselgenerierungsdienst	FCS_COP.1/SGD.ECDSA FCS_COP.1/SGD.Hash FCS_COP.1/SGD.ECIES FCS_COP.1/TSL.ECDSA FPT_TDC.1/SGD.Zert In O.ECIES wird gefordert: „Der TOE setzt das ECIES-Verfahren zur Gewährleistung der Integrität und Vertraulichkeit der Kommunikation mit dem Schlüsselgenerierungsdienst ein. Es verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [gemSpec_Krypt] und [gemSpec_SGD_ePA].“ Die zu übertragenen Daten werden nach FCS_COP.1/SGD.ECDSA authentifiziert, hierzu ist der Import des SGD-Zertifikats (vgl. FPT_TDC.1/SGD.Zert) notwendig, dieser wird nach der Anforderung aus FPT_TDC.1/SGD.Zert importiert. Dies erfordert gleichzeitig die Authentisierung und Verifikation der Zertifikate nach FCS_COP.1/TSL.ECDSA. Der eigentliche Schutz der Daten wird erfüllt durch die Verschlüsselungsfunktion, kompatibel zu den Anforderungen in FCS_COP.1/SGD.ECIES. Die Hashfunktion mit den Anforderungen FCS_COP.1/SGD.Hash gewährleistet die geforderte Integrität für das Protokoll.

Aspekt „Sicherer Kanal zum Schlüsselgenerierungsdienst“

In O.ECIES 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. Die Schlüsselvernichtung übernimmt FCS_CKM.4.

O.JWS

Aspekt des Ziels	SFR
JWS	FTP_ITC.1/JWS
	In O.JWS wird gefordert: „Der TOE setzt JSON Web Signature (JWS) ein zur Gewährleistung der Authentizität der ausgetauschten Daten ein.“ Genau dies leistet FTP_ITC.1/JWS.
Authentifizierung der übertragenen Daten	FCS_COP.1/JWS.ECDSA FCS_CKM.1/JWS.KEYS FCS_CKM.2/JWS.ECDSA
	In O.JWS wird gefordert: „Er verwendet dabei sichere kryptographische Algorithmen und Protokolle gemäß [TR-03107-1] mit den Einschränkungen der Atos Spezifikation für Kryptoalgorithmen [atosAuth1_V2].“ Um die Authentizität sicherzustellen wird ein kryptographisches Schlüsselpaar in FCS_CKM.1/JWS.KEYS erzeugt und der öffentliche Schlüssel über die Schlüsselverteilungsanforderung FCS_CKM.2/JWS.ECDSA an den Signaturdienst gegeben. Mit dem privaten Schlüssel signierte Daten können anschließend durch den Signaturdienst mit Hilfe des öffentlichen Schlüssels auf Authentizität geprüft werden. Die Signaturerzeugung wird mittels FCS_COP.1/JWS.ECDSA sicher gestellt.

O.Dok.Verschl

Aspekt des Ziels	SFR
Verschlüsselung der Dokumente	FCS_COP.1/AES
	Das Sicherheitsziel O.Dok.Verschl fordert, dass Dokumente des Versicherten nur symmetrisch verschlüsselt in die Dokumentenverwaltung eingestellt werden. Der zugehörige Dokumentenschlüssel wird mit dem Aktenschlüssel verschlüsselt in der Dokumentenverwaltung hinterlegt. Alle vom TOE verschlüsselten Dokumente und Schlüssel erfüllen die Anforderungen aus FCS_COP.1/AES.
Erzeugung der Schlüssel	FCS_CKM.1/Dok-Schlüssel
	Das Sicherheitsziel O.Dok.Verschl fordert, dass der Dokumentenschlüssel, Aktenschlüssel und Kontextschlüssel nach den Vorgaben aus [gemSpec_Krypt] erzeugt werden. FCS_CKM.1/Dok-Schlüssel erzwingt die Erzeugung auf die geforderte Art.

6.5. Erklärung für die gewählte EAL-Stufe

Die EAL-Stufe an sich ist in sich konsistent und erfüllt alle Abhängigkeiten. Die hier beschriebenen Vertrauenswürdigkeitskomponenten entsprechen den gewählten Vertrauenswürdigkeitskomponenten in Kapitel 6.3.

7. TOE Summary Specification

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.

Der Abschnitt 7.9 zeigt tabellarisch die Zusammenhänge zwischen den Sicherheitsfunktionen des TOE und den Sicherheitsanforderungen, die dieses Security Target in den Abschnitten 6.2 aufstellt.

7.1. Selbstschutz (SF.SelfProtection)

Die Sicherheitsfunktion SF.SelfProtection 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 Benutzerdaten. Das Löschen wird durch aktives Überschreiben der entsprechenden Speicherbereiche mit einer Konstante oder pseudo-zufälligen Werten umgesetzt.

Umgesetzte SFR
FDP_RIP.1

Der TOE schützt die ihm anvertrauten Daten. Diese Sicherheitsfunktion ist dafür verantwortlich, dass sensible Daten nur über die dafür vorgesehenen Schnittstellen den TOE verlassen.

Umgesetzte SFR
FPT_EMS.1

7.2. Kryptografische Dienste (SF.CryptographicServices)

Die Sicherheitsfunktion SF.CryptographicServices stellt Implementierungen verschiedener kryptographischer Basisalgorithmen zur Verfügung, die von anderen Sicherheitsfunktionen des TOE verwendet werden können.

Sicherer Datenspeicher

Der TOE unterstützt nur die symmetrische Verschlüsselung der Dokumente. Diese ist AES-basiert. Jedes Dokument wird mit dem zugehörigen Dokumentenschlüssel ver- bzw. entschlüsselt. Der Dokumentenschlüssel wird bei Dokumenten, die von der Dokumentenverwaltung bezogen werden, als mit dem Aktenschlüssel verschlüsseltes Chiffrat mit dem Dokument ausgeliefert. Beim Einstellen von neuen Dokumenten wird der Dokumentenschlüssel lokal erzeugt. Beim Aktivieren des Aktenkontos werden auch Akten- und Kontextschlüssel vom TOE erzeugt.

Alle kryptografischen Schlüssel werden, sobald sie nicht mehr benötigt werden, gelöscht. Das Löschen wird hier durch das Überschreiben der Daten mit Nullen umgesetzt.

Umgesetzte SFR	
FCS_CKM.1/Dok-Schlüssel	FCS_CKM.4

Symmetrische Verschlüsselung

Die Funktion bietet Implementierungen für die symmetrische Algorithmen zur Ver- und Entschlüsselung. Der TOE implementiert AES.

Umgesetzte SFR
FCS_COP.1/AES

Zufallszahlen

Der TOE enthält einen DRNG nach FCS_RNG.1, um Zufallszahlen hoher Qualität zu erzeugen. Der Seed für die Zufallszahlen wird aus der Systemzeit, Wisch-Bewegungen des Nutzers und dem Zufallszahlengenerator des Betriebssystems erzeugt. Die so erzeugten Zufallszahlen werden für verschiedene Zwecke verwendet, u.a. beim TLS-Verbindungsaufbau zur Erzeugung von Schlüsseln für das ECDHE-Verfahren (FCS_CKM.1/TLS)

Umgesetzte SFR
FCS_RNG.1

7.3. Trust-Service Status List (SF.TSL)

Der TOE verwendet zur Prüfung von TI-Zertifikaten eine Trust-Service Status List (TSL). Diese ist eine Liste von gegenwärtig gültigen Telematikinfrastruktur-Zertifikaten, die auch die Zertifikate selbst enthält. Der Aufbau ist in [gemSpec_TSL] dargestellt. Diese Liste wird vom Zugangsgateway heruntergeladen und lokal gespeichert. Innerhalb der TSL ist auch ein Gültigkeitszeitraum codiert, den der TOE auswertet. Ist dieser abgelaufen, muss eine neue TSL heruntergeladen werden. Zusätzlich wird überprüft, ob die heruntergeladene TSL bereits älter als 24 Stunden ist. Wenn innerhalb der letzten 24 Stunden keine Prüfung erfolgte, dann muss der TOE prüfen, ob eine neuere TSL zur Verfügung steht. Falls eine neuere TSL am Downloadpunkt bereit steht, so muss der TOE die neuere TSL herunterladen. Die heruntergeladene TSL wird vor jeder Verwendung kryptographisch auf Integrität und Authentizität geprüft. Dies geschieht durch Verifikation der Signatur mit dem TI-Vertrauensanker auf Basis von FCS_COP.1/TSL.ECDSA.

Umgesetzte SFR
FCS_COP.1/TSL.ECDSA

7.4. TLS-Service (SF.TLS)

Der TOE stellt die Umsetzung des TLS-Protokolls in der Version 1.2 und 1.3 bereit. Die Funktion stellt die Vertraulichkeit, Integrität und Authentizität der Verbindungen zum Zugangsgateway sicher. Die unterstützen Cipher-Suites und Kurven- Parameter finden sich in Anhang B. Die genaue Verwendung der

TLS-Verbindungen und eine Auflistung der Kommunikationspartner befindet sich in Tabelle Tabelle B.4.

Umgesetzte SFR
FTP_ITC.1/TLS

Um die Authentizität eines Zertifikats sicher zu stellen werden die Signaturen mittels des RSA oder ECDSA Verfahrens geprüft.

Umgesetzte SFR		
FCS_COP.1/TLS.Auth.RSA	FCS_COP.1/TLS.Auth.ECDSA	FCS_COP.1/TLS.Hash

Neben der Authentizitätsprüfung der Signatur eines Zertifikats muss geprüft werden ob das Zertifikat in einer gültigen Zertifikatskette zu einer zulässigen CA enthalten ist, das Zertifikat seine Gültigkeitsdauer überschritten hat oder mittels OCSP-Protokoll widerrufen wurde.

Umgesetzte SFR
FPT_TDC.1/TLS.Zert

Während des initialen Verbindungsaufbaus (TLS-Handshake) wird mittels des ECDHE-Verfahrens ein gemeinsames Geheimnis erzeugt und Schlüssel für die symmetrische Verschlüsselung abgeleitet.

Umgesetzte SFR
FCS_CKM.1/TLS

Für die Schlüsselableitung wird eine HKDF auf Basis von HMAC mit SHA-256 eingesetzt.

Umgesetzte SFR	
FCS_COP.1/TLS.HMAC	FCS_COP.1/TLS.Hash

Innerhalb des TLS-Handshakes wird ECDSA oder RSA verwendet um den Schlüsselaustausch zu authentifizieren.

Umgesetzte SFR	
FCS_COP.1/TLS.Auth.ECDSA	FCS_COP.1/TLS.Auth.RSA

Nach dem Handshake wird die Vertraulichkeit, Integrität und Authentizität der ausgetauschten Nachrichten durch AES-256 im GCM Modus gesichert.

Umgesetzte SFR
FCS_COP.1/TLS.AES

SHA-256 sowie SHA-384 wird bei der Prüfung von Zertifikaten eingesetzt sowie um die Integrität von Daten sicherzustellen. SHA-1 kommt ausschließlich im Zuge des OCSP-Protokolls zum Einsatz.

Umgesetzte SFR
FCS_COP.1/TLS.Hash

Für die Generierung von Nonces und Schlüsseln verwendet der TOE den Zufallsgenerator aus SF.CryptographicServices. Session Keys werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt, ebenfalls durch Aufruf von SF.CryptographicServices. Dabei werden auch die Funktionen in SF.CryptographicServices verwendet, die FCS_RNG.1 und FCS_CKM.4 realisieren.

7.5. VAU-Server-Protokoll (SF.VAU-Server-Protokoll)

Das VAU-Protokoll ist eine „leichtgewichtige Sicherungsschicht“, das von der gematik entwickelt wurde. Es dient zur Ende-zu-Ende-Verschlüsselung der Kommunikation zwischen dem TOE und der vertrauenswürdigen Ausführungsumgebung der Dokumentenverwaltung [gemSpec_Krypt, Kapitel 6]. Diese Zusammenfassung zeigt, welche SFR die Anforderungen aus den einzelnen Protokollschritten abdecken.

Umgesetzte SFR
FTP_ITC.1/VAU

7.5.1. 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. Das Zertifikat des TOE wird signiert und gehasht. Die Signatur wird dabei von der eGK oder dem Signaturdienst in der Umgebung des TOE erstellt. Der öffentliche Schlüssel des erzeugten Schlüsselpaars wird in der *VAUClientHello*-Nachricht an den VAU-Server gesendet.

Umgesetzte SFR	
FCS_CKM.1/VAU	FCS_COP.1/VAU.HASH

7.5.2. VAUServerHello

In Anforderung A_16903 wird gefordert, dass der TOE den Hashwert der vom VAU-Server erhaltenen *VAUServerHello*-Nachricht berechnet.

Umgesetzte SFR
FCS_COP.1/VAU.HASH

In Anforderung A_16941-01 wird gefordert, dass der Client das Zertifikat des Servers prüft. Dabei muss auch die Signatur des Zertifikats verifiziert werden. A_15873 [gemSpec_Frontend_Vers] definiert spezielle Prüfregeln für das Zertifikat, die der TOE ausführen muss. Auch hier wird der Hashwert berechnet.

Umgesetzte SFR		
FCS_COP.1/VAU.ECDSA	FPT_TDC.1/VAU.Zert	FCS_COP.1/VAU.HASH

7.5.3. ECDH-Schlüsselableitung

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.

Umgesetzte SFR
FCS_CKM.1/VAU

7.5.4. VAUClientSigFin

In Anforderung A_17070-01 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. Dabei wird die Funktionen in SF.CryptographicServices verwendet, die FCS_RNG.1 realisiert.

Umgesetzte SFR	
FCS_COP.1/VAU.AES	FCS_COP.1/VAU.HASH

7.5.5. Nutzerdatentransport

In Anforderung A_16945-01 wird gefordert, dass der TOE die Nutzerdaten ver- und entschlüsselt. Dies geschieht mit AES-GCM-256. Das zufällige Element des Initialisierungsvektors wird auch hier vom sicheren Zufallsgenerator erzeugt.

Umgesetzte SFR	
FCS_COP.1/VAU.AES	FCS_RNG.1

7.6. 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 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].

Umgesetzte SFR
FTP_ITC.1/SGD

7.6.1. Allgemeiner Protokollablauf

In diesem Abschnitt wird der allgemeine Protokollablauf und die dazu gehörenden Anforderungen auf die SFR aus Abschnitt 6.2.8 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 Schlüsselgenerierungsdienst.

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

7.6.1.1. 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 und prüft diese gemäß A_18024.

Umgesetzte SFR	
für a_17895-01:	FTP_ITC.1/SGD
für A_17897:	FTP_ITC.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

In den Schritten 9 (für SGD 1) und 14 (für SGD 2) fordert der TOE das Token über die Operation *GetAuthenticationToken* an. Die an den SGD-HSM zu übergebende Challenge wird mit dem sicheren Zufallsgenerator bestimmt. Dabei wird die Funktionen in SF.CryptographicServices verwendet, die FCS_RNG.1 realisiert. In den Nutzdaten des Requests wird der öffentliche ECIES-Schlüssel des TOEs übertragen. Die Nachricht wird nach dem ECIES-Verfahren verschlüsselt. Die Spezifikation definiert das in A_17875, wo die Schlüsselableitung mit ECDH und HKDF und die Verschlüsselung mit AES-GCM gefordert wird. Die Antwort des SGD-HSM wird entschlüsselt (Schritte 11 für SGD 1 und 16 für SGD 2) und die Hashwerte überprüft.

Umgesetzte SFR		
für A_17875:	FCS_COP.1/SGD.ECIES,	FCS_COP.1/SGD.ECDSA
für A_17902:	FCS_COP.1/SGD.ECIES	
für A_18028:	FCS_COP.1/SGD.Hash	

7.6.1.2. 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. Die Signatur des Schlüssels und der Hashwerte erfolgt gemäß A_17901 durch eine Karte oder AL.VI in der Umgebung des TOE und wird hier nicht durch einen SFR abgebildet.

Umgesetzte SFR	
für A_17900:	FCS_COP.1/SGD.Hash
für A_17874:	FCS_COP.1/SGD.ECIES
für A_17901:	Umgebung

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 gemäß A_18025 wird mit dem sicheren Zufallsgenerator bestimmt. In den Nutzdaten des Requests wird der öffentliche ECIES-Schlüssel des TOEs übertragen. Die Nachricht wird nach dem ECIES-Verfahren verschlüsselt. Die Spezifikation definiert das in A_17875, in der die Schlüsselableitung mit ECDH und HKDF und die Verschlüsselung mit AES-GCM gefordert wird. Die Antwort des SGD-HSM (gemäß A_18028) wird entschlüsselt (Schritte 11 für SGD 1 und 16 für SGD 2) und die Hashwerte überprüft.

Umgesetzte SFR		
für A_18021:	FTP_ITC.1/SGD	
für A_18025:	FCS_RNG.1	
für A_17875:	FCS_COP.1/SGD.ECIES,	FCS_COP.1/SGD.ECDSA
für A_17902:	FCS_COP.1/SGD.ECIES	
für A_18028:	FTP_ITC.1/SGD	
	FCS_COP.1/SGD.Hash	

7.6.1.3. 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[1]. Dazu verwendet der TOE gemäß A_17888 die Operation *KeyDerivation* des Schlüsselgenerierungsdienst (Schritt 12 für SGD 1 und 17 für SGD 2). A_18029 beschreibt den Aufbau der Nachricht. Der TOE erzeugt mit dem sicheren Zufallsgenerator eine Request ID, die er gemeinsam mit dem Authentisierungstoken aus dem vorherhigen Schritt ECIES-verschlüsselt und an den Schlüsselgenerierungsdienst sendet (Kodierung nach A_17902, ECIES wieder gemäß A_17875). Der TOE erhält die Daten ebenfalls verschlüsselt, er wendet das ECIES-Verfahren an, um die Nachricht des Servers zu entschlüsseln. Das Format der Nachricht ist in A_18031-01 definiert. Die entschlüsselten Nutzdaten enthalten den Berechtigungsschlüssel für den Zugriff auf das Aktensystem.

[1] 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.

Umgesetzte SFR		
für A_17888:	FTP_ITC.1/SGD	
für A_17898:	FTP_ITC.1/SGD	
für A_18029:	FTP_ITC.1/SGD	
	FCS_RNG.1	
für A_17875:	FCS_COP.1/SGD.ECIES,	FCS_COP.1/SGD.ECDSA
für A_17902:	FCS_COP.1/SGD.ECIES	
für A_17888:	FTP_ITC.1/SGD	

7.7. eGK Kommunikation (SF.EGK)

Der TOE schützt die Kommunikation über die kontaktlos-Schnittstelle des Geräts des Versicherten indem die Verbindung mit einem Secure Messaging Kanal geschützt wird.

Umgesetzte SFR
FTP_ITC.1/SM

Zur Erstellung des geschützten Kanals kommt das PACE Protokoll zum Einsatz.

Umgesetzte SFR
FCS_CKM.1/PACE

Dabei werden innerhalb des Protokolls symmetrische AES Sitzungsschlüssel generiert. Dazu wird auf Hash Algorithmen und CMAC zurückgegriffen.

Umgesetzte SFR		
FCS_CKM.1/SM	FCS_COP.1/SM.SHA	FCS_COP.1/SM.CMAC

Das Secure Messaging verwendet AES Schlüssel im CBC Modus. Session Keys werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt, durch Aufruf von SF.CryptographicServices.

Umgesetzte SFR
FCS_COP.1/SM.AES

7.8. SIGD Kommunikation (SF.SIGD)

Der TOE schützt die Kommunikation mit dem Signaturdienst durch TLS und JWS. Dies stellt die Authentizität, Integrität und Vertraulichkeit der Verbindung sicher. Für die erste Authentifizierung gebenüber dem Signaturdienst muss eine Verbindung mit dem Kontoverwaltungssystem hergestellt werden. Der TOE schützt dies Kommunikation ebenfalls durch einen TLS-Kanal. Das TLS-Protokoll wird durch SF.TLS implementiert.

Umgesetzte SFR
FTP_ITC.1/JWS

Nach dem TLS-Handshake wird die Vertraulichkeit, Integrität und Authentizität der ausgetauschten Nachrichten durch AES-256 im GCM Modus gesichert. Dabei wird die Funktion in SF.CryptographicServices verwendet die FCS_COP.1/AES realisiert.

Für die Generierung von Nonces und Schlüsseln in TLS verwendet der TOE den Zufallsgenerator aus SF.CryptographicServices. Session Keys werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt, ebenfalls durch Aufruf von SF.CryptographicServices. Es werden auch die Funktionen in SF.CryptographicServices verwendet die FCS_RNG.1 und FCS_CKM.4 realisieren.

Um das verwendete Gerät gegenüber dem Kontoverwaltungssystem zu authentifizieren wird Commitment-Verfahren auf Basis von SHA256 verwendet.

Umgesetzte SFR
FCS_COP.1/OAUTH.HASH

Während des initialen Verbindungsaufbaus mit dem Signaturdienst wird ein Schlüsselpaar durch den TOE erzeugt (FCS_CKM.1/JWS.KEYS) und der öffentliche Teil dieses Schlüsselpaares vom TOE an den Signaturdienst einmalig übertragen (FCS_CKM.2/JWS.ECDSA). Die Authentizität dieser initialen Übertragung wird über ein vorher vom Signaturdienst bezogenes Anmeldetoken sichergestellt, die Integrität der Kommunikation wird über eine Signatur der Daten (FCS_COP.1/JWS.ECDSA) mit dem privaten Schlüssel aus FCS_CKM.1/JWS.KEYS gewährleistet.

Umgesetzte SFR	
FCS_CKM.1/JWS.KEYS	FCS_CKM.2/JWS.ECDSA

Das Schlüsselpaar wird anschließend in JWS verwendet, um den TOE gegenüber dem Signaturdienst in allen weiteren Aufrufen zu authentifizieren. Dafür signiert der TOE (siehe FCS_COP.1/JWS.ECDSA) die zu übertragenden Daten mit dem nur ihm bekannten privaten Teil des Schlüsselpaars aus FCS_CKM.1/JWS.KEYS. Der Signaturdienst prüft die Integrität und Authentizität der erhaltenen Daten anschließend mit dem ihm initial übermittelten öffentlichen Teil des Schlüsselpaars aus FCS_CKM.1/JWS.KEYS.

Umgesetzte SFR
FCS_COP.1/JWS.ECDSA

7.9. Verhältnis von SFR zu SF

Tabelle 7.1 zeigt, in welchem Verhältnis die im Abschnitt Abschnitt 6.2 definierten Sicherheitsanforderungen an den TOE zu den in Abschnitt 7 beschriebenen Sicherheitsfunktionen stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	SF.CryptographicServices	SF.EGK	SF.SelfProtection	SF.SGD	SF.SIGD	SF.TLS	SF.TSL	SF.VAU-Server-Protokoll
FCS_CKM.1/Dok-Schlüssel	✓	.	.	.	.	.	.	.
FCS_CKM.1/SM	.	✓	.	.	.	.	.	.
FCS_CKM.1/PACE	.	✓	.	.	.	.	.	.
FCS_CKM.1/TLS	.	.	.	.	.	✓	.	.
FCS_CKM.1/VAU	.	.	.	.	.	.	.	✓
FCS_CKM.1/JWS.KEYS	.	.	.	.	✓	.	.	.
FCS_CKM.2/JWS.ECDSA	.	.	.	.	✓	.	.	.
FCS_CKM.4	✓	.	.	.	.	.	.	.
FCS_COP.1/AES	✓	.	.	.	.	.	.	.
FCS_COP.1/JWS.ECDSA	.	.	.	.	✓	.	.	.
FCS_COP.1/OAUTH.HASH	.	.	.	.	✓	.	.	.
FCS_COP.1/SGD.ECDSA	.	.	.	✓	.	.	.	.
FCS_COP.1/SGD.Hash	.	.	.	✓	.	.	.	.
FCS_COP.1/SGD.ECIES	.	.	.	✓	.	.	.	.
FCS_COP.1/SM.AES	.	✓	.	.	.	.	.	.
FCS_COP.1/SM.CMAC	.	✓	.	.	.	.	.	.
FCS_COP.1/SM.SHA	.	✓	.	.	.	.	.	.
FCS_COP.1/TLS.AES	.	.	.	.	.	✓	.	.
FCS_COP.1/TLS.Auth.ECDSA	.	.	.	.	.	✓	.	.
FCS_COP.1/TLS.Auth.RSA	.	.	.	.	.	✓	.	.
FCS_COP.1/TLS.Hash	.	.	.	.	.	✓	.	.
FCS_COP.1/TLS.HMAC	.	.	.	.	.	✓	.	.
FCS_COP.1/TSL.ECDSA	.	.	.	.	.	.	✓	.
FCS_COP.1/VAU.AES	.	.	.	.	.	.	.	✓
FCS_COP.1/VAU.ECDSA	.	.	.	.	.	.	.	✓
FCS_COP.1/VAU.HASH	.	.	.	.	.	.	.	✓
FCS_RNG.1	✓	.	.	.	.	.	.	.
FDP_ACC.1/SGD	.	.	.	✓	.	.	.	.
FDP_ACF.1/SGD	.	.	.	✓	.	.	.	.
FDP_ITC.2/SGD	.	.	.	✓	.	.	.	.
FDP_RIP.1	.	.	✓	.	.	.	.	.
FPT_EMS.1	.	.	✓	.	.	.	.	.

Tabelle 7.1.: Abbildung der SFR auf Sicherheitsfunktionalität

	SF.CryptographicServices	SF.EGK	SF.SelfProtection	SF.SGD	SF.SIGD	SF.TLS	SF.TSL	SF.VAU-Server-Protokoll
FPT_TDC.1/TLS.Zert	.	.	.	.	.	✓	.	.
FPT_TDC.1/SGD.Zert	.	.	.	✓	.	.	.	.
FPT_TDC.1/VAU.Zert	.	.	.	.	.	.	.	✓
FTP_ITC.1/SGD	.	.	.	✓	.	.	.	.
FTP_ITC.1/SM	.	✓	.	.	.	.	.	.
FTP_ITC.1/TLS	.	.	.	.	.	✓	.	.
FTP_ITC.1/VAU	.	.	.	.	.	.	.	✓
FTP_ITC.1/JWS	.	.	.	.	✓	.	.	.

Tabelle 7.1.: Abbildung der SFR auf Sicherheitsfunktionalität

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
✓	Vorgesehene Beziehung zwischen SFR und SF

Tabelle A.1.: Legende der Abbildungstabellen

B. TLS Verbindungen

Der TOE beherrscht die in Tabelle B.1 aufgeführten Cipher Suiten und kann darüber hinaus Cipher Suiten aus [TR-02102-2] unterstützen. 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 1.3 [RFC 8446]
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_256_GCM_SHA384	`0xc0,0x2C`	✓	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	`0xc0,0x2B`	✓	
TLS_AES_128_GCM_SHA256	`0x13,0x01`		✓

Tabelle B.1.: Cipher Suites der TLS Verbindungen des TOE

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 5639; RFC 7027]
brainpoolP384r1	`27`	[RFC 5639; RFC 7027]

Tabelle B.2.: Elliptische Kurven für die TLS Verbindungen des TOE

Der TOE kommuniziert mit anderen vertrauenswürdigen TI-Produkten über gesicherte Verbindungen. Die Integrität und die Vertrauenswürdigkeit der Verbindungen wird durch die Verwendung von TLS in der Version 1.2 oder 1.3 und die in Tabelle B.1 genannten Algorithmen und Cipher Suiten sichergestellt. Tabelle B.4 listet die Verbindungen auf, die der TOE eingeht. Die Spalten dieser Tabelle werden in Tabelle B.3 beschrieben.

Spalte	Beschreibung
ID	Symbolischer Name der Verbindung
Schnittstelle	Logische Schnittstelle des TOE , über die die Verbindung läuft.
Rolle	Beschreibt, ob der TOE in dieser Verbindung Client oder Server ist.
Peer	Beschreibung des Partners in der TLS-Verbindung
Protokoll	Anwendungsprotokoll, das für die Verbindung genutzt wird.
Subsystem::Modul	Name des Subsystems und des Moduls, von dem die Verbindung ausgeht, bzw. das die Verbindung empfängt und behandelt.
Port	Port, den der TOE öffnet, um die Verbindung aufzubauen. Für Verbindungen, bei denen der TOE 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.
Identität des TOE	Zertifikat, mit dem sich der TOE gegenüber dem Peer authentisiert.
Identität des Peer	Zertifikat/Verfahren, mit dem sich der Peer gegenüber dem TOE authentisiert.
Authentifizierung des Peer durch	Verfahren, Datenquelle oder Subsystem/Modul, mit dem der TOE die Identität des Peers verifiziert.

Tabelle B.3.: Legende zu den TLS Verbindungen

ID	Schnittstelle (Protokoll)	Rolle	Peer	Subsystem::Modul	Port	Identität des TOE	Identität des Peer	Authentifizierung des Peer durch
TLS.1	LS.GATEWAY	Client	Gateway	C++-Core::OpenSSL	443	-	Internet-Zertifikat	ePA-Modul Frontend des Versicherten
TLS.2	LS.SIGNATURDIENST	Client	SigD	C++-Core::OpenSSL	443	-	Internet-Zertifikat	ePA-Modul Frontend des Versicherten
TLS.3	LS.KVS	Client	KVS	C++-Core::OpenSSL	443	-	Internet-Zertifikat	ePA-Modul Frontend des Versicherten

Tabelle B.4.: TLS Verbindungen des ePA Modul FdV

Literatur

gematik Spezifikationen

[gemProdTePAModulFdV] gematik GmbH. *Produkttypsteckbrief des ePAFrontends des Versicherten*. Prüfvorschrift. Produkttyp Version PTV1 1.1.0-0. Version 1.0.0., 5. Nov. 2020.

[gemSpec_AuthentisierungVers] gematik GmbH. *Spezifikation Authentisierung des Versicherten ePA*. Spezifikation. Version 1.2.0., 2. März 2020.

[gemSpec_Autorisierung] gematik GmbH. *Spezifikation Autorisierung ePA*. Version 1.4.2. Revision 271577., 27. Aug. 2020.

[gemSpec_COS] gematik GmbH. *Spezifikation des Card Operating System (COS)*. Version 3.13.1. Revision 177507., 1. Nov. 2019.

[gemSpec_DMePA] gematik GmbH. *Datenmodell ePA*. Spezifikation. Version 1.4.2. 271579., 27. Aug. 2020.

[gemSpec_Dokumentenverwaltung] gematik GmbH. *Spezifikation ePA-Dokumentenverwaltung*. Spezifikation. Version 1.4.2. 271581., 27. Aug. 2020.

[gemSpec_Frontend_Vers] gematik GmbH. *Sepzifikation ePA-Frontend des Versicherten*. Spezifikation. Version 1.5.2. Revision 273070., 27. Aug. 2020.

[gemSpec_FrontendVersUEePA] gematik GmbH. *Addendum zur Spezifikation ePA-Frontend des Versicherten*. Spezifikation. Version 1.2.0., 2. März 2020.

[gemSpec_Krypt] gematik GmbH. *Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur*. Version 2.16.2. Revision 293627xs., 5. Nov. 2020.

[gemSpec_OID] gematik GmbH. *Spezifikation Festlegung von OIDs*. Version 3.7.1. Revision 277093., 18. Sep. 2020.

[gemSpec_PKI] gematik GmbH. *Übergreifende Spezifikation PKI*. Version 2.8.1. Revision 245775., 26. Juni 2020.

[gemSpec_SGD_ePA] gematik GmbH. *Spezifikation Schlüsselgenerierungsdienst ePA*. Version 1.4.1. Revision 293956., 5. Nov. 2020.

[gemSpec_SystemprozessedezTI] gematik GmbH. *Spezifikation Systemprozesse der dezentralen TI*. Spezifikation. Version 1.2.0., 28. Juni 2019.

[gemSpec_TSL] gematik GmbH. *Spezifikation TSL-Dienst*. Version 1.17.0. Revision 198519., 2. März 2020.

[gemSpec_Zugangsgateway_Vers] gematik GmbH. *Spezifikation Zugangsgateway des Versicherten ePA*. Spezifikation. Version 1.4.1., 26. Juni 2020.

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 3268] P. Chown. *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*. RFC 3268 (Proposed Standard). RFC. Obsoleted by RFC 5246. Fremont, CA, USA: RFC Editor, Juni 2002. DOI: 10.17487/RFC3268. URL: https://www.rfc-editor.org/rfc/rfc3268.txt.

[RFC 4492] S. Blake-Wilson u. a. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*. RFC 4492 (Informational). RFC. Updated by RFCs 5246, 7027, 7919. Fremont, CA, USA: RFC Editor, Mai 2006. DOI: 10.17487/RFC4492. URL: https://www.rfc-editor.org/rfc/rfc4492.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 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 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 6749] D. Hardt (Ed.) *The OAuth 2.0 Authorization Framework*. RFC 6749 (Proposed Standard). RFC. Updated by RFC 8252. Fremont, CA, USA: RFC Editor, Okt. 2012. DOI: 10.17487/RFC6749. URL: https://www.rfc-editor.org/rfc/rfc6749.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 7515] Michael Jones, John Bradley und Nat Sakimura. *JSON Web Signature (JWS)*. RFC 7515. Mai 2015. DOI: 10.17487/RFC7515. URL: https://www.rfc-editor.org/rfc/rfc7515.txt.

[RFC 7636] N. Sakimura (Ed.), J. Bradley und N. Agarwal. *Proof Key for Code Exchange by OAuth Public Clients*. RFC 7636 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Sep. 2015. DOI: 10.17487/RFC7636. URL: https://www.rfc-editor.org/rfc/rfc7636.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.

[RFC 8446] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2018. DOI: 10.17487/RFC8446. URL: https://www.rfc-editor.org/rfc/rfc8446.txt.

Andere

[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.

[atosAuth1_V2] Atos Information Technology GmbH. *Elektronische Identifizierungsmittel vom Sicherheitsniveau substanziell. Authentifizierungsvariante 1*. Spezifikation. Version V2. Atos Information Technology GmbH, 2020.

[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, Sep. 2012. 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, Sep. 2012. URL: http://www.commoncriteriaportal.org/thecc.html.

[cgmKontoverwaltung_V2.3] CompuGroup Medical Software GmbH. *CGM LIFE ePA Kontoverwaltung. CGM LIFE Inventory als Kontoverwaltungssystem*. Spezifikation. Version 2.3. CompuGroup Medical Software GmbH, 1. Okt. 2020.

[FIPS PUB 180-4] National Institute of Standards und Technology. *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Aug. 2015. URL: http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[FIPS PUB 186-4] 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 PUB 197] National Institute of Standards und Technology. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Nov. 2001. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[ISO 7816-4] *Identification cards — Integrated circuit cards — Part 4: Interindustry commands for interchange*. en. Standard ISO/IEC TR 7816-4:2013. Geneva, CH: International Organization for Standardization, Apr. 2013. URL: https://www.iso.org/standard/54550.html.

[NIST SP 800-133 Rev. 2] Elaine Barker und Allen Roginsky. *Recommendation for Cryptographic Key Generation*. NIST Special Publication 800-133 Rev.2. National Institute of Standards und Technology, Juni 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf.

[NIST SP 800-38A] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. Methods and Techniques*. NIST Special Publication 800-38A. National Institute of Standards und Technology, Dez. 2001. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf.

[NIST SP 800-38B] 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, Dez. 2001. URL: http://nvlpubs.nist.gov/

nistpubs/Legacy/SP/nistspecialpublication800-38b.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 800-56-A] 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. National Industrial Security Program Operating Manual*. NIST Special Publication. Version Revision 1. National Institute of Standards und Technology, Juni 2015. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.

[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.

[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/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.

[TR-02102-2] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS)*. Technische Richtlinie BSI TR-02102-2. Technical Guideline. Version 2018-01. Bundesamt für Sicherheit in der Informationstechnik (BSI), 15. Dez. 2017. URL: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.

[TR-03107-1] Bundesamt für Sicherheit in der Informationstechnik. *Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1: Vertrauensniveaus und Mechanismen*. Technische Richtlinie BSI TR-03107-1. Technical Guideline. Version 1.1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 7. Mai 2019. URL: https://www.bsi.bund.de/

SharedDocs / Downloads / DE / BSI / Publikationen / TechnischeRichtlinien/TR03107/TR-03107-1.html.

[TR-03110-2] Bundesamt für Sicherheit in der Informationstechnik. *Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS)*. Technische Richtlinie BSI TR-03110. Technical Guideline. Version 2.21. Bundesamt für Sicherheit in der Informationstechnik (BSI), 28. Aug. 2012. URL: https : / / www . bsi . bund . de / EN / Publications / TechnicalGuidelines/TR03110/BSITR03110.html.

[TR-03111] Bundesamt für Sicherheit in der Informationstechnik. *Elliptic Curve Cryptography*. Technische Richtlinie BSI TR-03111. Technical Guideline. Version 2.9. Bundesamt für Sicherheit in der Informationstechnik (BSI), 28. Aug. 2012. URL: https : / / www . bsi . bund . de / DE / Publikationen / TechnischeRichtlinien/tr03111/index_htm.html.

[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.

Verzeichnis der ST-Anwendungshinweise

Index der SFR