

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Highspeed-Konnektor

Produkttyp Version: 1.3.0-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 670029
Stand: 10.07.2023
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_Kon_Highspeed_PTV_1.3.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die normativen Festlegungen für den Produkttyp ändern und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version auf Dokumentenebene	gemProdT_Kon_Highspeed_PTV1.0.0-0
1.1.0-0	Anpassung durch HSK_Maintenance_22.1 (und Konn_Maintenance_22.1)	gemProdT_Kon_Highspeed_PTV1.1.0-0
1.2.0-0	Anpassung durch Konn_Maintenance_22.2 - 22.6 und gemF_TI-Gateway	gemProdT_Kon_Highspeed_PTV1.2.0-0
1.2.1-0	Anpassung durch Konn_Maintenance_23.0	gemProdT_Kon_Highspeed_PTV1.2.1-0
1.3.0-0	Anpassung durch HSK_Maintenance_23.0 - _23.1	gemProdT_Kon_Highspeed_PTV1.3.0-0

Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	10.07.23		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung	4
1.1 Zielsetzung und Einordnung des Dokumentes	4
1.2 Zielgruppe	4
1.3 Geltungsbereich	4
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik	5
2 Dokumente	6
3 Normative Festlegungen	9
3.1 Festlegungen zur funktionalen Eignung.....	9
3.1.1 Produkttest/Produktübergreifender Test	9
3.1.2 Herstellererklärung funktionale Eignung	61
3.2 Festlegungen zur sicherheitstechnischen Eignung	78
3.2.1 Beschleunigte Sicherheitszertifizierung (BSZ)	78
3.2.2 Prüfung durch CC-Prüfstelle.....	82
3.2.3 Produktgutachten	98
3.2.4 Sicherheitsgutachten	99
3.2.5 Herstellererklärung sicherheitstechnische Eignung.....	107
3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	116
4 Produkttypspezifische Merkmale	117
4.1 Leistungsstufen	117
4.2 Ausprägungsformen des Konnektors	117
4.3 Optionale Ausprägungen	117
4.3.1 Option IPv6	117
4.4 Referenzdokumente	118
5 Anhang A – Verzeichnisse	119
5.1 Abkürzungen	119
5.2 Tabellenverzeichnis	119
5.3 Referenzierte Dokumente	120

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps Konnektor oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik. (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.)

Die normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die normativen Festlegungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an Konnektor-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- akkreditierten Materialprüflaboren
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich normative Festlegungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. gemPTV_ATV_Festlegungen, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für den Anbietertyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten normativen Festlegungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativer Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativer Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

Normative Festlegungen, die im Titel den Zusatz „ab PTV4“ haben, gelten ab der Produkttypversion 4 des Konnektors. Sie ersetzen normative Festlegungen mit gleicher ID (ohne Suffix), die für die Produkttypversionen 1 bis 3 gültig waren.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen. Hierbei gelten auch Festlegungen an den Konnektor, die an einen Consumer oder ein Consumer-Fachmodul gerichtet sind.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemSpec_FM_ePA	Spezifikation Fachmodul ePA	1. 44 53.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.1 45 .40
gemSpec_SST_FD_VSDM	Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1. 67 .0
gemSpec_SST_VSDM	Schnittstellenspezifikation Transport VSDM	2.5.0
gemSpec_TSL	Spezifikation TSL-Dienst	1. 49 20.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.2 68 .0
gemSpec_FM_AMTS	Spezifikation Fachmodul AMTS	1.4.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.1 01 .20
gemSpec_PINPUK_TI	Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0
gemSpec_eGK_Fach_VSDM	Speicherstrukturen der eGK für die Fachanwendung VSDM	1.2.1
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.2 34 .0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.1 45 .40
gemSpec_VZD	Spezifikation Verzeichnisdienst	1.15.0
gemSpec_Info_AMTS	Informationsmodell eMP/AMTS-Datenmanagement	1.5.0
gemSpec_KT	Spezifikation eHealth-Kartenterminal	3.16.0
gemSpec_Karten_Fach_TIP_G2_1	Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3. 01 .0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.1 45 .21
gemSpec_FM_NFDM	Spezifikation Fachmodul NFDM	1.6.2
gemSpec_eGK_Fach_NFDM	Speicherstrukturen der eGK für die Fachanwendung NFDM	1.1.0
gemSpec_gSMC-K_ObjSys	Spezifikation der gSMC-K Objektsystem	3.14.0

gemSpec_Dokumentenverwaltung	Spezifikation Dokumentenverwaltung ePA	1. 44 54.1
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.2 69 .20
gemF_Highspeed-Konnektor	Feature Spezifikation Highspeed-Konnektor 2.0	1.42.0
gemSpec_Authentisierung_Vers	Spezifikation Authentisierung des Versicherten ePA	1.6.0
gemSpec_Kon	Spezifikation Konnektor	5. 48 20.0
gemSpec_KSR	Spezifikation Konfigurationsdienst	2. 56 .40
gemSpec_SST_PS_VSDM	Schnittstellenspezifikation Primärsysteme VSDM	1.5.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1. 45 .0
gemSpec_eGK_Fach_AMTS	Speicherstrukturen der eGK für die Fachanwendung AMTS	1.2.0
gemSpec_SGD_ePA	Spezifikation Schlüsselgenerierungsdienst ePA	1. 56 .0
gemSpec_DM_ePA	Datenmodell ePA	1. 40 53.1
gemSpec_InfoNFDM	Informationsmodell Notfalldaten-Management (NFDM)	1. 67 .0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.5.0
gemKPT_Test	Testkonzept der TI	2.8. 67
gemSpec_FM_VSDM	Spezifikation Fachmodul VSDM	2. 78 .0
gemSpec_TBAuth	Übergreifende Spezifikation Tokenbasierte Authentisierung	1.2.0
gemF_TI-Gateway	Feature TI-Gateway	1.0.0
gemSpec_SMC_OPT	Gemeinsame optische Merkmale der SMC	3.8.0

Tabelle 2: Mitgeltende Dokumente

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
[gemRL_QES_NFDM]	Signaturrichtlinie QES Notfalldaten-Management (NFDM)	1.4
[gemSpec_OID]	Spezifikation Festlegung von OIDs	3.14.0
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung	2.2.0

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
[AIS_B_HSK]	AIS B HSK - Anwendungshinweise und Interpretationen zum Schema (AIS) - Anforderungen an einen Highspeed-Konnektor, BSI	0.93

Die Festlegungen zum BSZ-Geltungsbereich HSK finden in einem AIS-Dokument des BSI statt [AIS_B_HSK].

Tabelle 3 enthält die kompatiblen Versionen der Repositories in GitHub.

Tabelle 3: GitHub Repository-Links

GitHub Repository	Branch / Tag	URL
api-telematik	OPB4 / 4.1.3	https://github.com/gematik/api-telematik/tree/4.1.3
api-ePA	master / 2.1.1	https://github.com/gematik/api-ePA/tree/2.1.1

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Festlegungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

Tabelle 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

ID	Bezeichnung	Quelle (Referenz)
A_21854	Nutzung des VSDM-Intermediärs	gemF_Highspeed-Konnektor
A_22338	Tägliche Aktualisierung der TSL	gemF_Highspeed-Konnektor
A_23258	Rollenausschlüsse Highspeedkonnektor	gemF_IIHighspeed-GatKonnewayktor
A_23303	TLS mit Client-Authentisierung verpflichtend für Clientsystemanbindungen	gemF_IIHighspeed-GatKonnewayktor
A_23359	Administration des HSK-Basis Systems	gemF_IIHighspeed-GatKonnewayktor
A_23397	Sicherung und Wiederherstellung HSK-Basissystem	gemF_IIHighspeed-GatKonnewayktor
A_23432	Verpflichtendes Auto-Update	gemF_IIHighspeed-GatKonnewayktor
A_23444	Verifikation gesteckter SMC-B	gemF_IIHighspeed-GatKonnewayktor
A_23446	Messung von Verfügbarkeitsdaten	gemF_IIHighspeed-GatKonnewayktor
A_23469	Unterstützung AK.AUT und individuelle Identität an der Management-Schnittstelle	gemF_IIHighspeed-GatKonnewayktor

ID	Bezeichnung	Quelle (Referenz)
A_23477	Protokollierung Infomodell - Clientsysteme	gemF_Highspeed-Konnektor
A_23478	HSK, http-Forwarder - Absenderadresse	gemF_Highspeed-Konnektor
A_23480	Anonymisierung	gemF_Highspeed-Konnektor
A_23488	HSK, http-Forwarder - Funktion	gemF_Highspeed-Konnektor
A_23761	Highspeed-Konnektor:Betriebsdaten - Bereitstellung von Betriebsdaten - Basissystem	gemF_Highspeed-Konnektor
A_23762	Highspeed-Konnektor:Betriebsdaten - Fehlerbehandlung	gemF_Highspeed-Konnektor
A_23763	Highspeed-Konnektor:Betriebsdaten - contentUploadXML nicht vorhanden	gemF_Highspeed-Konnektor
A_23769	Highspeed-Konnektor:Betriebsdaten - Konfiguration Betriebsstättenart	gemF_Highspeed-Konnektor
A_23846	Highspeed-Konnektor:Betriebsdaten - Konfiguration CI-ID	gemF_Highspeed-Konnektor
A_23847	Highspeed-Konnektor:Betriebsdaten - Konfiguration URL Schnittstelle ContentUploadXML	gemF_Highspeed-Konnektor
A_23857	Highspeed-Konnektor:Betriebsdaten - Vermeiden von Spitzenlasten beim Senden von Betriebsdaten	gemF_Highspeed-Konnektor
A_23882	HSK OCSP-Adressierung	gemF_Highspeed-Konnektor
GS-A_3829-01	HSK: Nutzung externer Namensräume	gemF_Highspeed-Konnektor
TIP1-A_4503-03	Verpflichtung zur Nutzung von gSMC-K oder HSM	gemF_Highspeed-Konnektor
TIP1-A_4693-03	TUC_KON_032 „TSL aktualisieren“	gemF_Highspeed-Konnektor
TIP1-A_4701-03	TUC_KON_035 „Zertifikatsdienst initialisieren“	gemF_Highspeed-Konnektor
TIP1-A_4730-02	Kommunikation mit NET_TI_GESICHERTE_FD	gemF_Highspeed-Konnektor
TIP1-A_4731-02	Kommunikation mit NET_TI_ZENTRAL	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4732-02	Kommunikation mit NET_TI_DEZENTRAL	gemF_Highspeed-Konnektor
TIP1-A_4733-02	Kommunikation mit ANLW_AKTIVE_BESTANDSNETZE	gemF_Highspeed-Konnektor
TIP1-A_4793-02	Konfigurierbarkeit des Konnektor NTP-Servers (Highspeed-Konnektor)	gemF_Highspeed-Konnektor
TIP1-A_4795-03	TUC_KON_352 „Initialisierung Zeitdienst“ (Highspeed-Konnektor)	gemF_Highspeed-Konnektor
TIP1-A_4797-03	HSK: DNS-Forwards des DNS-Servers	gemF_Highspeed-Konnektor
TIP1-A_4805-02	HSK: Konfigurationsparameter Namensdienst und Dienstlokalisierung	gemF_Highspeed-Konnektor
TIP1-A_4810-02	Benutzerverwaltung der Managementschnittstelle	gemF_Highspeed-Konnektor
TIP1-A_4814-02	Export- Import von Konfigurationsdaten	gemF_Highspeed-Konnektor
TIP1-A_4832-03	TUC_KON_280 „Konnektoraktualisierung durchführen“	gemF_Highspeed-Konnektor
A_14682-02	Entschlüsselung eines Dokuments beim Herunterladen aus der Dokumentenverwaltung	gemSpec_DM_ePA
A_14961-05	Nutzungsvorgaben für die Verwendung von XDS-Metadaten bei Policy Documents	gemSpec_DM_ePA
A_14974	Nutzungsvorgabe für DocumentEntry.patientId und SubmissionSet.patientId	gemSpec_DM_ePA
A_14975-01	Verschlüsselung des Dokuments mit dem DocumentKey	gemSpec_DM_ePA
A_14976-02	Verschlüsselung des DocumentKey mit dem RecordKey	gemSpec_DM_ePA
A_14977-02	Dokumentenverschlüsselung gemäß XML Encryption	gemSpec_DM_ePA
A_21200	Komponente ePA-Dokumentenverwaltung und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten	gemSpec_Dokumentenverwaltung
AMTS-A_2134	FM AMTS: Zurückverfolgbarkeit von Fehlern	gemSpec_FM_AMTS
AMTS-A_2142	FM AMTS: Fachmodulprotokoll (Fehler)	gemSpec_FM_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2143	FM AMTS: Sicherheitsprotokoll	gemSpec_FM_AMTS
AMTS-A_2144	FM AMTS: Fachmodulprotokoll (Ablauf)	gemSpec_FM_AMTS
AMTS-A_2150	FM AMTS: Erzeugung von Zugriffsprotokolleinträgen für eGK G2.1	gemSpec_FM_AMTS
AMTS-A_2151	FM AMTS: Format der Zugriffsprotokolleinträge des Fachmoduls AMTS auf der eGK G2.0	gemSpec_FM_AMTS
AMTS-A_2152	FM AMTS: Übergreifende Konfigurationsparameter	gemSpec_FM_AMTS
AMTS-A_2153	FM AMTS: Registrierung im Dienstverzeichnis des Konnektors	gemSpec_FM_AMTS
AMTS-A_2154	FM AMTS: AMTS_Service	gemSpec_FM_AMTS
AMTS-A_2157	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei fehlenden Smartcards	gemSpec_FM_AMTS
AMTS-A_2158	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei nicht freigeschalteten Smartcards	gemSpec_FM_AMTS
AMTS-A_2159	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei falschen Aufrufparametern	gemSpec_FM_AMTS
AMTS-A_2160	FM AMTS: Übergreifende Anforderung – Zugriffsberechtigung auf benötigte Ressourcen	gemSpec_FM_AMTS
AMTS-A_2161	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei fehlender Zugriffsberechtigung	gemSpec_FM_AMTS
AMTS-A_2162	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei gesperrter Gesundheitsanwendung auf der eGK	gemSpec_FM_AMTS
AMTS-A_2163	FM AMTS: Übergreifende Anforderung – Prüfung von Authentizität und Echtheit der beteiligten Smartcards (C2C)	gemSpec_FM_AMTS
AMTS-A_2165	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei falscher eGK-Version	gemSpec_FM_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2166	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei inkonsistentem Datensatz	gemSpec_FM_AMTS
AMTS-A_2167	FM AMTS: Übergreifende Anforderung – Keine Nutzung der Privat-PIN	gemSpec_FM_AMTS
AMTS-A_2168	FM AMTS: Übergreifende Anforderung – Caching der Versicherten-ID während einer Karten-Session für eGK G2.0	gemSpec_FM_AMTS
AMTS-A_2170	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei nicht aktivierter Fachanwendung eMP/AMTS auf der eGK	gemSpec_FM_AMTS
AMTS-A_2172	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei eGK-Sperrung	gemSpec_FM_AMTS
AMTS-A_2173	FM AMTS: Übergreifende Anforderung – Durchgeführte Operationen bei eGK-Sperrung	gemSpec_FM_AMTS
AMTS-A_2174	FM AMTS: Übergreifende Anforderung – Befüllung des Rückgabeparameters EGKValid	gemSpec_FM_AMTS
AMTS-A_2175	FM AMTS: Übergreifende Anforderung – Befüllung des Rückgabeparameters Status	gemSpec_FM_AMTS
AMTS-A_2178	FM AMTS: Übergreifende Anforderung – Operationen abrechnen	gemSpec_FM_AMTS
AMTS-A_2179	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung beim vorzeitigen Ziehen der eGK	gemSpec_FM_AMTS
AMTS-A_2180	FM AMTS: Meldungen am Kartenterminal	gemSpec_FM_AMTS
AMTS-A_2181	FM AMTS: Terminalanzeige für PIN-Eingaben	gemSpec_FM_AMTS
AMTS-A_2182	FM AMTS: GrantApproval – Prüfung auf Einwilligung beim Zugriff auf die eMP/AMTS-Daten (Einverständnis)	gemSpec_FM_AMTS
AMTS-A_2183	FM AMTS: GrantApproval – Fehlerbehandlung bei Prüfung des Einverständnisses	gemSpec_FM_AMTS
AMTS-A_2185	FM AMTS: ReadMP – Daten von eGK lesen	gemSpec_FM_AMTS
AMTS-A_2187	FM AMTS: ReadMP – Daten dekomprimieren und kodieren	gemSpec_FM_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2188	FM AMTS: ReadMP – Vollständigkeit der eMP/AMTS-Daten	gemSpec_FM_AMTS
AMTS-A_2191	FM AMTS: ReadMP – Befüllung des Rückgabeparameters EGKUsage	gemSpec_FM_AMTS
AMTS-A_2193	FM AMTS: WriteMP – Daten auf eGK schreiben	gemSpec_FM_AMTS
AMTS-A_2195	FM AMTS: WriteMP – Vollständigkeit der eMP/AMTS-Daten	gemSpec_FM_AMTS
AMTS-A_2197	FM AMTS: WriteMP – Fehlerbehandlung bei abweichender Versicherten-ID	gemSpec_FM_AMTS
AMTS-A_2198	FM AMTS: WriteMP – Fehlerbehandlung bei fehlerhaften Parametern	gemSpec_FM_AMTS
AMTS-A_2200	FM AMTS: WriteMP – eMP/AMTS-Daten komprimieren und dekodieren	gemSpec_FM_AMTS
AMTS-A_2201	FM AMTS: WriteMP – Fehlerbehandlung bei nicht ausreichendem Speicherplatz	gemSpec_FM_AMTS
AMTS-A_2203	FM AMTS: ReadConsent – Daten von eGK lesen	gemSpec_FM_AMTS
AMTS-A_2204	FM AMTS: Zugriff auf die Einwilligung nur mit AMTS-PIN	gemSpec_FM_AMTS
AMTS-A_2205	FM AMTS: WriteConsent – Daten auf die eGK schreiben	gemSpec_FM_AMTS
AMTS-A_2206	FM AMTS: DeleteConsent – Einwilligung löschen	gemSpec_FM_AMTS
AMTS-A_2207	FM AMTS: DeleteConsent – Sicherheitsabfrage zur Löschung der Einwilligung	gemSpec_FM_AMTS
AMTS-A_2208	FM AMTS: DeleteConsent – Bestätigung der Löschung	gemSpec_FM_AMTS
AMTS-A_2209	FM AMTS: DeleteConsent – Abbruch des Löschvorgangs	gemSpec_FM_AMTS
AMTS-A_2238	FM AMTS: Übergreifende Anforderung – Transaktionsstatus setzen	gemSpec_FM_AMTS
AMTS-A_2643	FM AMTS: Ein einziger Zugriffsprotokolleintrag pro Kartensitzung mit eGK G2.0	gemSpec_FM_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2646	FM AMTS: Übergreifende Anforderung – paralleler Zugriff	gemSpec_FM_AMTS
AMTS-A_2647	FM AMTS: Übergreifende Anforderung – Überspringen des Caching der Versicherten-ID für eGK G2.0	gemSpec_FM_AMTS
AMTS-A_2688	FM AMTS: Performanceprotokoll	gemSpec_FM_AMTS
A_17823	FM AMTS: ReadMP - Fehlerbehandlung bei leerem Datensatz	gemSpec_FM_AMTS
NFDM-A_2086	Web Services konform zu [BasicProfile1.2]	gemSpec_FM_NFDM
NFDM-A_2089	Protokollierung inkl. Trace-Struktur	gemSpec_FM_NFDM
NFDM-A_2090	Transport Fehlermeldungen als gematik-SOAP-Fault	gemSpec_FM_NFDM
NFDM-A_2091	Zurückverfolgbarkeit von Fehlerketten	gemSpec_FM_NFDM
NFDM-A_2092	Vorgaben spezifische Fehlermeldungen	gemSpec_FM_NFDM
NFDM-A_2093	Verfügbarkeit Transportsicherung	gemSpec_FM_NFDM
NFDM-A_2094	Unterstützte Generationen der eGK	gemSpec_FM_NFDM
NFDM-A_2099	Fachmodulprotokoll (Fehler)	gemSpec_FM_NFDM
NFDM-A_2100	Sicherheitsprotokoll (SecurityLog)	gemSpec_FM_NFDM
NFDM-A_2101	Fachmodulprotokoll (Ablauf)	gemSpec_FM_NFDM
NFDM-A_2102	Performanceprotokoll	gemSpec_FM_NFDM
NFDM-A_2104	Übergreifende Konfigurationsparameter	gemSpec_FM_NFDM
NFDM-A_2106	Service-Informationen für Dienstverzeichnisdienste	gemSpec_FM_NFDM
NFDM-A_2107	Meldungen am Kartenterminal	gemSpec_FM_NFDM
NFDM-A_2108	Terminalanzeigen für PIN-Eingabe	gemSpec_FM_NFDM
NFDM-A_2109	NFDSservice	gemSpec_FM_NFDM
NFDM-A_2110	Operation ReadNFD	gemSpec_FM_NFDM
NFDM-A_2112	Berechtigungsregeln ReadNFD	gemSpec_FM_NFDM
NFDM-A_2113	Operation WriteNFD	gemSpec_FM_NFDM

ID	Bezeichnung	Quelle (Referenz)
NFDM-A_2115	Berechtigungsregeln WriteNFD	gemSpec_FM_NFDM
NFDM-A_2116-01	Operation EraseNFD	gemSpec_FM_NFDM
NFDM-A_2118	Berechtigungsregeln EraseNFD	gemSpec_FM_NFDM
NFDM-A_2119	DPEService	gemSpec_FM_NFDM
NFDM-A_2120	Operation ReadDPE	gemSpec_FM_NFDM
NFDM-A_2122	Berechtigungsregeln ReadDPE	gemSpec_FM_NFDM
NFDM-A_2123	Operation WriteDPE	gemSpec_FM_NFDM
NFDM-A_2125	Berechtigungsregeln WriteDPE	gemSpec_FM_NFDM
NFDM-A_2126-01	Operation EraseDPE	gemSpec_FM_NFDM
NFDM-A_2128	Berechtigungsregeln EraseDPE	gemSpec_FM_NFDM
NFDM-A_2135	Zugriffsprotokollierung auf der eGK	gemSpec_FM_NFDM
NFDM-A_2371	Zusammenfassung mehrerer Protokolleinträge mittels Vorgangsnummer	gemSpec_FM_NFDM
NFDM-A_2382	Nutzung der Signaturrichtlinie NFDM	gemSpec_FM_NFDM
NFDM-A_2406	Protokollierung	gemSpec_FM_NFDM
A_23020	Vorrang von gesperrter eGK	gemSpec_FM_VSDM
A_23157	Vorrang von ungültigem Zertifikat	gemSpec_FM_VSDM
A_23158	Vorrang von gesperrtem Zertifikat	gemSpec_FM_VSDM
A_23959	HSK-Fachmodul VSDM: Ermitteln der URL des VSDM Intermediärs	gemSpec_FM_VSDM
VSDM-A_2563	Fachmodul VSDM: Abbruch nach Timeout	gemSpec_FM_VSDM
VSDM-A_2565	Fachmodul VSDM: parallele Verarbeitung	gemSpec_FM_VSDM
VSDM-A_2566	Fachmodul VSDM: konfigurierbare Parameter	gemSpec_FM_VSDM
VSDM-A_2567	ReadVSD: VD, PD und Status-Container lesen	gemSpec_FM_VSDM
VSDM-A_2568	ReadVSD: gesperrte Gesundheitsanwendung	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2569	ReadVSD: AUT-Zertifikat der eGK offline ungültig	gemSpec_FM_VSDM
VSDM-A_2570	ReadVSD: AUT-Zertifikat der eGK online ungültig	gemSpec_FM_VSDM
VSDM-A_2571	ReadVSD: technischer Fehler	gemSpec_FM_VSDM
VSDM-A_2572	ReadVSD: GVD in Antwort enthalten	gemSpec_FM_VSDM
VSDM-A_2573	ReadVSD: Echtheitsprüfung eGK	gemSpec_FM_VSDM
VSDM-A_2574	ReadVSD: Echtheitsprüfung SM-B/HBA	gemSpec_FM_VSDM
VSDM-A_2575	ReadVSD: Prüfungsnachweis wenn erstellt	gemSpec_FM_VSDM
VSDM-A_2576	ReadVSD: Prüfungsnachweis von der eGK, wenn möglich	gemSpec_FM_VSDM
VSDM-A_2577	ReadVSD: Prüfungsnachweis lesen	gemSpec_FM_VSDM
VSDM-A_2578-01	ReadVSD: Prüfungsnachweis erzeugen	gemSpec_FM_VSDM
VSDM-A_2579	ReadVSD: Prüfungsnachweis schreiben	gemSpec_FM_VSDM
VSDM-A_2580	Fachmodul VSDM: ReadVSD - Aktualisierungsaufträge ermitteln	gemSpec_FM_VSDM
VSDM-A_2581	ReadVSD: Aktualisierung durchführen	gemSpec_FM_VSDM
VSDM-A_2582	ReadVSD: Aktualisierungsaufträge ermitteln wegen gesperrter Gesundheitsanwendung	gemSpec_FM_VSDM
VSDM-A_2583	ReadVSD: Aktualisierungsaufträge ermitteln wegen offline ungültigem AUTH-Zertifikat	gemSpec_FM_VSDM
VSDM-A_2584	ReadVSD: Aktualisierungsaufträge ermitteln wegen online ungültigem AUTH-Zertifikat	gemSpec_FM_VSDM
VSDM-A_2585	ReadVSD: Aktualisierung CMS	gemSpec_FM_VSDM
VSDM-A_2586	ReadVSD: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2587	ReadVSD: Protokollierung GVD Lesen	gemSpec_FM_VSDM
VSDM-A_2588	Fachmodul VSDM: Prüfungsnachweis erstellen	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2589-01	Fachmodul VSDM: Prüfungsnachweis-Ergebnis erstellen	gemSpec_FM_VSDM
VSDM-A_2590	Fachmodul VSDM: Prüfungsnachweis komprimieren	gemSpec_FM_VSDM
VSDM-A_2591	Fachmodul VSDM: Prüfungsnachweis verschlüsseln	gemSpec_FM_VSDM
VSDM-A_2592	Fachmodul VSDM: Prüfungsnachweis entschlüsseln	gemSpec_FM_VSDM
VSDM-A_2594	Fachmodul VSDM: Variante - Prüfungsnachweis nicht vorhanden.	gemSpec_FM_VSDM
VSDM-A_2595	Fachmodul VSDM: Variante - Prüfungsnachweis nicht entschlüsselbar	gemSpec_FM_VSDM
VSDM-A_2597	Fachmodul VSDM: Aktualisierungsaufträge ermitteln	gemSpec_FM_VSDM
VSDM-A_2601	Fachmodul VSDM: Aktualisierungsaufträge durchführen	gemSpec_FM_VSDM
VSDM-A_2602	Fachmodul VSDM: Reihenfolge der Abarbeitung der Aktualisierungsaufträge	gemSpec_FM_VSDM
VSDM-A_2603	Fachmodul VSDM: Separate Aktualisierungen für mehrere UpdateIds	gemSpec_FM_VSDM
VSDM-A_2604	ReadVSD: Fehlermeldung wenn Gesundheitsanwendung im Ablauf gesperrt wird	gemSpec_FM_VSDM
VSDM-A_2605	ReadVSD: Keine Fehlermeldung wenn Gesundheitsanwendung im Ablauf entsperrt wird	gemSpec_FM_VSDM
VSDM-A_2606	Fachmodul VSDM: Abbruch aller weiteren Aktualisierungen bei Fehler in einer Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2607	Fachmodul VSDM: alte Versionen der eGK	gemSpec_FM_VSDM
VSDM-A_2609	ReadKVK: Versichertendaten	gemSpec_FM_VSDM
VSDM-A_2611	ReadKVK: Abbruch bei fehlgeschlagener Prüfung	gemSpec_FM_VSDM
VSDM-A_2612	Fachmodul VSDM: Umsetzung des Anwendungsfalls "VSDM-UC_02: Automatische Onlineprüfung VSD"	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2613	Fachmodul VSDM: Aufruf der Operation AutoUpdateVSD	gemSpec_FM_VSDM
VSDM-A_2614-01	AutoUpdateVSD: Prüfungsnachweis erzeugen	gemSpec_FM_VSDM
VSDM-A_2615	AutoUpdateVSD: Prüfungsnachweis schreiben	gemSpec_FM_VSDM
VSDM-A_2616	Fachmodul VSDM: AutoUpdateVSD - Texte für Anzeige am Kartenterminal	gemSpec_FM_VSDM
VSDM-A_2619	AutoUpdateVSD: Aktualisierungsaufträge ermitteln	gemSpec_FM_VSDM
VSDM-A_2620	AutoUpdateVSD: Aktualisierung durchführen	gemSpec_FM_VSDM
VSDM-A_2621	AutoUpdateVSD: Echtheitsprüfung eGK	gemSpec_FM_VSDM
VSDM-A_2622	AutoUpdateVSD: Echtheitsprüfung SMC-B/HBA	gemSpec_FM_VSDM
VSDM-A_2623	AutoUpdateVSD: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2624	AutoUpdateVSD: Fehlermeldung wenn Gesundheitsanwendung im Ablauf gesperrt wird	gemSpec_FM_VSDM
VSDM-A_2625	AutoUpdateVSD: Keine Fehlermeldung wenn Gesundheitsanwendung im Ablauf entsperrt wird	gemSpec_FM_VSDM
VSDM-A_2626	ReadKVK: Ablauf des Gültigkeitsdatums	gemSpec_FM_VSDM
VSDM-A_2636	Fachmodul VSDM: Protokollierung im einheitlichen Format	gemSpec_FM_VSDM
VSDM-A_2638	Fachmodul VSDM: Felder im Ablaufprotokoll	gemSpec_FM_VSDM
VSDM-A_2639	Fachmodul VSDM: Felder im Performance-Protokoll	gemSpec_FM_VSDM
VSDM-A_2642	Fachmodul VSDM: Verarbeitungszeiten anderer Systeme im Performance-Protokoll	gemSpec_FM_VSDM
VSDM-A_2649	Fachmodul VSDM: Protokolldateien begrenzen auf 180 Tage, Datenschutz	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2650	Fachmodul VSDM: Vorgangsnummer bilden	gemSpec_FM_VSDM
VSDM-A_2651	Fachmodul VSDM: Felder im Fehler-Protokoll	gemSpec_FM_VSDM
VSDM-A_2652	ReadVSD: Daten base64-kodiert	gemSpec_FM_VSDM
VSDM-A_2653	Fachmodul VSDM: Prüfungsnachweis - ErrorCode	gemSpec_FM_VSDM
VSDM-A_2654	Fachmodul VSDM: Abbruch wenn Protokoll nicht auf eGK geschrieben	gemSpec_FM_VSDM
VSDM-A_2655	Fachmodul VSDM: Prüfungsnachweis überschreiben	gemSpec_FM_VSDM
VSDM-A_2660	ReadVSD: inkonsistente VSD	gemSpec_FM_VSDM
VSDM-A_2662	ReadVSD: Abbruch C2C wenn Aktualisierungen vorliegen	gemSpec_FM_VSDM
VSDM-A_2664	Fachmodul VSDM: Ereignisdienst - maximale Offlinezeit überschritten	gemSpec_FM_VSDM
VSDM-A_2667	Fachmodul VSDM: Ereignisdienst - Texte für Fortschritt	gemSpec_FM_VSDM
VSDM-A_2668	Fachmodul VSDM: Endpunkt-Adresse des Intermediärs bilden	gemSpec_FM_VSDM
VSDM-A_2687	Fachmodul VSDM: unterstützte Versionen der eGK	gemSpec_FM_VSDM
VSDM-A_2708	Fachmodul VSDM: Werte für StatusVD in Antwortnachricht	gemSpec_FM_VSDM
VSDM-A_2745	Fachmodul VSDM: Schlüssel für Prüfungsnachweis mandantenfähig ablegen	gemSpec_FM_VSDM
VSDM-A_2749	Fachmodul VSDM: zugehörige Nachrichten zum Fehler	gemSpec_FM_VSDM
VSDM-A_2752	Fachmodul VSDM: Aktualisierungsaufträge einzeln ausführen	gemSpec_FM_VSDM
VSDM-A_2770	Fachmodul VSDM: Prüfungsnachweis minimieren	gemSpec_FM_VSDM
VSDM-A_2772	ReadVSD: Prüfungsnachweis parallelisiert schreiben	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2775	ReadVSD: Aufrufkontext prüfen	gemSpec_FM_VSDM
VSDM-A_2776	Fachmodul VSDM: Schlüssel aus Eingabe ableiten	gemSpec_FM_VSDM
VSDM-A_2777	Fachmodul VSDM: Schlüssel und Prüfungsnachweis mandantenfähig	gemSpec_FM_VSDM
VSDM-A_2778	Fachmodul VSDM: Anzeige Masterschlüssel	gemSpec_FM_VSDM
VSDM-A_2779	Fachmodul VSDM: Masterschlüssel zufällig erzeugen	gemSpec_FM_VSDM
VSDM-A_2784	ReadVSD: GVD nicht aus dem Container EF.VD lesen	gemSpec_FM_VSDM
VSDM-A_2791	Fachmodul VSDM: Ausführungszeiten im Performance-Protokoll	gemSpec_FM_VSDM
VSDM-A_2792	Fachmodul VSDM: ReadVSD in den Dienstverzeichnisdienst einbringen	gemSpec_FM_VSDM
VSDM-A_2793	Fachmodul VSDM: ReadKVK in den Dienstverzeichnisdienst einbringen	gemSpec_FM_VSDM
VSDM-A_2944	Fachmodul VSDM: Debugprotokoll schreiben	gemSpec_FM_VSDM
VSDM-A_2979	Fachmodul VSDM: unterstützte Versionen der VSDM Speicherstrukturen auf der eGK	gemSpec_FM_VSDM
VSDM-A_2981	Fachmodul VSDM: Kartenterminal - Texte für Fortschritt	gemSpec_FM_VSDM
VSDM-A_2989	Fachmodul VSDM: Speicherstruktur des Containers EF.Prüfungsnachweises auf der eGK	gemSpec_FM_VSDM
VSDM-A_2998	Fachmodul VSDM: Abbruch der Operation ReadVSD	gemSpec_FM_VSDM
VSDM-A_3020	Fachmodul VSDM: Konfiguration des Context zum Aufruf der Operation AutoUpdateVSD	gemSpec_FM_VSDM
VSDM-A_3033	Fachmodul VSDM: kein Prüfungsnachweis wenn Online nicht aktiviert	gemSpec_FM_VSDM
VSDM-A_3067	Prüfungsnachweis protokollieren	gemSpec_FM_VSDM
VSDM-A_3070-01	Kassenspezifischen Teil der ICCSN der eGK im Fehlerprotokoll speichern	gemSpec_FM_VSDM

ID	Bezeichnung	Quelle (Referenz)
A_13784-01	FM ePA: GetHomeCommunityID - Keine Akte - Fehler	gemSpec_FM_ePA
A_13785-01	FM ePA: GetHomeCommunityID - Zwei oder mehr Akten - Fehler	gemSpec_FM_ePA
A_13786-01	FM ePA: GetHomeCommunityID - Eine Akte	gemSpec_FM_ePA
A_13818-06	FM ePA: PHRManagementService Version 2.0.1	gemSpec_FM_ePA
A_13828-05	FM ePA: Service-Informationen für Dienstverzeichnisdienste	gemSpec_FM_ePA
A_13839	FM ePA: Lokalisierung - ePA-Aktensystem und Komponenten	gemSpec_FM_ePA
A_13907	FM ePA: putDocuments - Verschlüsselung der Dokumente	gemSpec_FM_ePA
A_13941	FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen	gemSpec_FM_ePA
A_13964	FM ePA: PHRService - SOAP Security Header	gemSpec_FM_ePA
A_14014	FM ePA: Autorisierung Aktensession - Request SAML	gemSpec_FM_ePA
A_14024-02	FM ePA: Autorisierung Aktensession - Fehler	gemSpec_FM_ePA
A_14025	FM ePA: Lokalisierung - ePA-Aktensystem und Komponenten - Fehler	gemSpec_FM_ePA
A_14084	FM ePA: Login - Bereitstellung Default-Aufrufkontext	gemSpec_FM_ePA
A_14103	FM ePA: Login - Konfiguration Default-Aufrufkontext	gemSpec_FM_ePA
A_14105	FM ePA: Autorisierung - TLS-Verbindung zur Komponente Autorisierung aufbauen	gemSpec_FM_ePA
A_14107-03	FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen - Fehler	gemSpec_FM_ePA
A_14156	FM ePA: Einheitliches Log-Format	gemSpec_FM_ePA
A_14157	FM ePA: Korrelation von Log-Einträgen	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_14221	FM ePA: Übergreifende Anforderung - Unterstützte Generationen der eGK - Fehler	gemSpec_FM_ePA
A_14222	FM ePA: Autorisierung - Verwendung der lokalisierten URI	gemSpec_FM_ePA
A_14223	FM ePA: Autorisierung - Verbindung mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_14241	FM ePA: Übergreifende Anforderung - Unterstützte Generationen der eGK	gemSpec_FM_ePA
A_14243	FM ePA: Autorisierung Aktensession - Fehler - keine Autorisierung vorhanden	gemSpec_FM_ePA
A_14266	FM ePA: PHRManagementService - Befüllung des Rückgabeparameters Status	gemSpec_FM_ePA
A_14271	FM ePA: ActivateAccount - Terminalanzeige für PIN-Eingaben der Operation	gemSpec_FM_ePA
A_14353	FM ePA: putDocuments - Gruppierung von IHE-Akteuren	gemSpec_FM_ePA
A_14354	FM ePA: Übergreifende Anforderung IHE - Keine Prüfung der Metadaten-Profilierung	gemSpec_FM_ePA
A_14373-08	FM ePA: PHRService Version 2.x	gemSpec_FM_ePA
A_14376	FM ePA: PHRService - Fehlermeldungen gemäß IHE	gemSpec_FM_ePA
A_14377-01	FM ePA: PHRService - Fehlermeldungen gemäß IHE-Mapping	gemSpec_FM_ePA
A_14400	FM ePA: Übergreifende Anforderung - Server nicht erreichbar - Fehler	gemSpec_FM_ePA
A_14405	FM ePA: Übergreifende Anforderung - Fehlermeldungen des Webservice PHRManagementService (SOAP-Fault)	gemSpec_FM_ePA
A_14406	FM ePA: Übergreifende Anforderung - Allgemeine Fehlerbehandlung	gemSpec_FM_ePA
A_14412	FM ePA: Übergreifende Anforderung - Unterstützung unbekannter Generationen der eGK	gemSpec_FM_ePA
A_14414	FM ePA: Übergreifende Anforderung - Fehlende Smartcard	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_14586-01	FM ePA: GetHomeCommunityID - Schnittstelle zur Abfrage am ePA-Aktensystem	gemSpec_FM_ePA
A_14647	FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts	gemSpec_FM_ePA
A_14649	FM ePA: Dokumentenverwaltung - Verwendung des Kontextschlüssels	gemSpec_FM_ePA
A_14650-01	FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts - Fehler in der Dokumentenverwaltung	gemSpec_FM_ePA
A_14700	FM ePA: getDocuments - Entschlüsselung der Dokumente	gemSpec_FM_ePA
A_14711	FM ePA: Fachmodulprotokoll	gemSpec_FM_ePA
A_14712	FM ePA: Fachmodul-Performance-Protokoll	gemSpec_FM_ePA
A_14749	FM ePA: ActivateAccount - Hinterlegen des verschlüsselten Schlüsselmaterials	gemSpec_FM_ePA
A_14759	FM ePA: Übergreifende Anforderung - Gesperrter Ordner DF.HCA auf der eGK	gemSpec_FM_ePA
A_14767	FM ePA: Übergreifende Anforderung - Gesperrtes Zertifikat auf der eGK	gemSpec_FM_ePA
A_14769	FM ePA: RequestFacilityAuthorization - Bestätigung der Berechtigung	gemSpec_FM_ePA
A_14829	FM ePA: RequestFacilityAuthorization - Hinterlegen des verschlüsselten Schlüsselmaterials in der Komponente Autorisierung	gemSpec_FM_ePA
A_14833	FM ePA: RequestFacilityAuthorization - Ablage der Policy-Dokumente in der Dokumentenverwaltung	gemSpec_FM_ePA
A_14834-01	FM ePA: RequestFacilityAuthorization - Berechtigungen in Dokumentenverwaltung einbringen - Fehler im Aktensystem	gemSpec_FM_ePA
A_14838	FM ePA: Authentisierung mit eGK - Authentifizierungsbestätigung erstellen	gemSpec_FM_ePA
A_14874	FM ePA: PHRService - Mapping für Fehlerkategorie "Fatal"	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_14927	FM ePA: Authentisierung mit SM-B - Erstellung des SAML-Token	gemSpec_FM_ePA
A_14928	FM ePA: Authentisierung mit eGK - PIN-Eingabe	gemSpec_FM_ePA
A_14929	FM ePA: Authentisierung mit eGK - TLS-Verbindung zur Komponente Zugangsgateway aufbauen	gemSpec_FM_ePA
A_14930	FM ePA: Authentisierung mit eGK - TLS mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_14935	FM ePA: Authentisierung mit eGK - Fehler im Aktensystem	gemSpec_FM_ePA
A_14945-01	FM ePA: Authentisierung mit eGK - PIN-Eingabe - Fehler	gemSpec_FM_ePA
A_14947	FM ePA: Login - Ermittlung des Aufrufkontexts via Aufrufparameter	gemSpec_FM_ePA
A_14948	FM ePA: Login - Verwendung des Default-Aufrufkontexts bei fehlenden SOAP-Headern	gemSpec_FM_ePA
A_15134-02	FM ePA: Autorisierung Aktensession - Benachrichtigung an das Primärsystem	gemSpec_FM_ePA
A_15137	FM ePA: Übergreifende Anforderung - Unterbindung paralleler Zugriffe auf die eGK - Fehler	gemSpec_FM_ePA
A_15142-02	FM ePA: Login - Ermittlung des Aufrufkontexts via SOAP-Header - PHRService Version 2.x	gemSpec_FM_ePA
A_15191	FM ePA: PHRService - Authentisierung mittels SM-B	gemSpec_FM_ePA
A_15192	FM ePA: PHRManagementService - Authentisierung mittels eGK	gemSpec_FM_ePA
A_15193	FM ePA: PHRManagementService - Authentisierung mittels SM-B	gemSpec_FM_ePA
A_15199-01	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Verfahren	gemSpec_FM_ePA
A_15200	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Aufrufparameter	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_15210	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_15211	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Fehler	gemSpec_FM_ePA
A_15216	FM ePA: Übergreifende Anforderung - Fehlerbehandlung bei nicht erfolgreicher C2C-Prüfung	gemSpec_FM_ePA
A_15228-01	FM ePA: GetHomeCommunityID - Anfrage an alle bekannten ePA-Aktensysteme	gemSpec_FM_ePA
A_15531-04	FM ePA: Dokumentenverwaltung - TLS-Verbindung zur Komponente Dokumentenverwaltung aufbauen	gemSpec_FM_ePA
A_15532	FM ePA: Dokumentenverwaltung - TLS mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_15533	FM ePA: Dokumentenverwaltung - Verwendung der lokalisierten URI	gemSpec_FM_ePA
A_15575	FM ePA: Übergreifende Anforderung - SOAP für Webservices	gemSpec_FM_ePA
A_15614-01	FM ePA: Übergreifende Anforderung - Ermittlung eines SM-B	gemSpec_FM_ePA
A_15615-03	FM ePA: Übergreifende Anforderung - Mandant nicht ePA-fähig - Fehler	gemSpec_FM_ePA
A_15626	FM ePA: PHRService - Ver- und Entschlüsselung von Dokumenten - Fehler	gemSpec_FM_ePA
A_15638	FM ePA: Authentisierung mit SM-B - Behauptungen im SAML-Token	gemSpec_FM_ePA
A_15647	FM ePA: Übergreifende Anforderung - Konfigurationsparameter des Fachmoduls ePA	gemSpec_FM_ePA
A_15648	FM ePA: Übergreifende Anforderung - Timeout bei TLS-Verbindungs Aufbau - Fehler	gemSpec_FM_ePA
A_15649	FM ePA: Übergreifende Anforderung - Aktensystem antwortet nicht - Fehler	gemSpec_FM_ePA
A_15675	FM ePA: Übergreifende Anforderung - Syntaxprüfung bei Aufrufen von Webservices - Fehler	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_15693	FM ePA: RequestFacilityAuthorization - Erstellung von Policy Document	gemSpec_FM_ePA
A_15693-05	FM ePA: RequestFacilityAuthorization Version 2.x - Erstellung von Policy Document	gemSpec_FM_ePA
A_15763	FM ePA: PHR_Service: Weiterleiten einer putDocuments-Anfrage	gemSpec_FM_ePA
A_15764	FM ePA: PHR_Service: Weiterleiten von putDocuments-Antwort	gemSpec_FM_ePA
A_15765	FM ePA: PHR_Service: Weiterleiten einer find-Anfrage	gemSpec_FM_ePA
A_15766	FM ePA: PHR_Service: Weiterleiten von find-Antworten	gemSpec_FM_ePA
A_15767	Weiterleiten einer getDocuments-Anfrage an das ePA-Aktensystem	gemSpec_FM_ePA
A_15768	FM ePA: PHR_Service: Weiterleiten von getDocuments-Antworten	gemSpec_FM_ePA
A_15769-02	FM ePA: PHR_Service: Weiterleiten einer removeDocuments-Anfrage	gemSpec_FM_ePA
A_15770-01	FM ePA: PHR_Service: Weiterleiten von removeDocuments-Antwort	gemSpec_FM_ePA
A_16193	FM ePA: Übergreifende Anforderung - Vorgaben Aktenschlüssel und Kontextschlüssel - Fehler	gemSpec_FM_ePA
A_16207-01	FM ePA: PHRService - Maximale Größe aller Dokumente	gemSpec_FM_ePA
A_16208-01	FM ePA: PHRService - Maximale Größe aller Dokumente - Fehler	gemSpec_FM_ePA
A_16209-02	FM ePA: PHRService - Maximale Größe eines Dokuments	gemSpec_FM_ePA
A_16210-01	FM ePA: PHRService - Maximale Größe eines Dokuments - Fehler	gemSpec_FM_ePA
A_16211	FM ePA: Übergreifende Anforderung - Zertifikat auf der eGK nicht prüfbar	gemSpec_FM_ePA
A_16212-07	FM ePA: RequestFacilityAuthorization Version 2.x - Anzeige am Kartenterminal - Anzeigetext	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_16214-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Bestätigung	gemSpec_FM_ePA
A_16215-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Abbruch	gemSpec_FM_ePA
A_16216-01	FM ePA: RequestFacilityAuthorization - Terminalanzeige für PIN-Eingaben der Operation	gemSpec_FM_ePA
A_16218-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Nutzerinteraktion	gemSpec_FM_ePA
A_16219-02	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Optimierung	gemSpec_FM_ePA
A_16220-01	FM ePA: Übergreifende Anforderung IHE - Dokumenten-Codierung	gemSpec_FM_ePA
A_16351	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Mapping von InsurantName und OrganizationName	gemSpec_FM_ePA
A_16352	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - nicht darstellbare Zeichen von InsurantName und OrganizationName	gemSpec_FM_ePA
A_16951	FM ePA: Authentisierung mit eGK-Verwendung der lokalisierten URI	gemSpec_FM_ePA
A_17120	FM ePA: RequestFacilityAuthorization - Berechtigungen in Dokumentenverwaltung einbringen - Fehler	gemSpec_FM_ePA
A_17121-01	FM ePA: PHRManagementService - Berechtigung in Komponente Autorisierung - Fehler	gemSpec_FM_ePA
A_17123	FM ePA: Authentisierung mit eGK - Fehler beim Aufruf Aktensystem	gemSpec_FM_ePA
A_17133	FM ePA: PHRManagementService - Statusprüfung Aktenkonto - Fehler	gemSpec_FM_ePA
A_17142	FM ePA: Logout Aktensession - Löschung der Verbindung zur VAU - Fehler	gemSpec_FM_ePA
A_17167	FM ePA: GetAuthorizationList - Anfrage an alle bekannten ePA-Aktensysteme	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_17174	FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten	gemSpec_FM_ePA
A_17175	FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten - Fehler	gemSpec_FM_ePA
A_17177	FM ePA: GetAuthorizationList - Erstellung der RecordIdentifier	gemSpec_FM_ePA
A_17213	FM ePA: Bedingte Kontoaktivierung - Aufruf der Operation ActivateAccount	gemSpec_FM_ePA
A_17214-01	FM ePA: Bedingte Kontoaktivierung - Event FM_EPA/ACTIVATE_ACCOUNT/START	gemSpec_FM_ePA
A_17215-01	FM ePA: Bedingte Kontoaktivierung - Event FM_EPA/ACTIVATE_ACCOUNT/FINISHED	gemSpec_FM_ePA
A_17219	FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten - Warnung	gemSpec_FM_ePA
A_17227	FM ePA: Übergreifende Konfigurationsparameter	gemSpec_FM_ePA
A_17228	FM ePA: Fachmodulprotokoll (Fehler)	gemSpec_FM_ePA
A_17229-01	FM ePA: Fachmodulprotokoll (Debug)	gemSpec_FM_ePA
A_17230	FM ePA: Sicherheitsprotokoll	gemSpec_FM_ePA
A_17231	FM ePA: Performanceprotokoll	gemSpec_FM_ePA
A_17437	FM ePA: RequestFacilityAuthorization - SOAP-Security-Header	gemSpec_FM_ePA
A_17450-01	FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion	gemSpec_FM_ePA
A_17451	FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion - Fehler	gemSpec_FM_ePA
A_17483	FM ePA: Übergreifende Anforderung - Kryptographische Verfahren für Smartcards der Generation 2	gemSpec_FM_ePA
A_17484	FM ePA: Übergreifende Anforderung - Kryptographische Verfahren für Smartcards ab Generation 2.1	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_17736	FM ePA: Schlüsselableitung bei Entschlüsselung - Fehler bei der Entschlüsselung	gemSpec_FM_ePA
A_17743	FM ePA: ActivateAccount - Akten- und Kontextschlüssel für den Versicherten verschlüsseln	gemSpec_FM_ePA
A_17744-03	FM ePA: Übergreifende Anforderung - Status des Aktenkontos - Fehlerbehandlung	gemSpec_FM_ePA
A_17765	FM ePA: GetHomeCommunityID - Abfrage eines Aktenkontos nicht möglich	gemSpec_FM_ePA
A_17767	FM ePA: GetAuthorizationList - Abfrage der Berechtigung einer einzelnen Akte nicht möglich	gemSpec_FM_ePA
A_17868	FM ePA: RequestFacilityAuthorization - Akten- und Kontextschlüssel mit eGK verschlüsseln	gemSpec_FM_ePA
A_17869	FM ePA: Schlüsselableitung bei Entschlüsselung - Entschlüsselung mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_17870	FM ePA: Schlüsselableitung - Fehler im Schlüsselgenerierungsdienst	gemSpec_FM_ePA
A_17871	FM ePA: Schlüsselableitung - Fehler an der Schnittstelle zum Schlüsselgenerierungsdienst	gemSpec_FM_ePA
A_17948	FM ePA: Authentisierung mit eGK - TLS-Verbindung - Fehler	gemSpec_FM_ePA
A_17949-01	FM ePA: Aktensession - Löschen der Aktensession bei Entfernen der eGK	gemSpec_FM_ePA
A_17966	FM ePA: Schlüsselableitung - Ablauf	gemSpec_FM_ePA
A_17986	FM ePA: Schlüsselableitung bei Entschlüsselung- Abhängigkeit von der Rolle	gemSpec_FM_ePA
A_17988	FM ePA: RequestFacilityAuthorization - Schlüsselableitung in Abhängigkeit von der Rolle	gemSpec_FM_ePA
A_17992	FM ePA: Schlüsselableitung - Ermittlung von AssociatedData	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_17993	FM ePA: Schlüsselableitung bei Entschlüsselung - Verwendung von AssociatedData	gemSpec_FM_ePA
A_18007	Schlüsselableitung bei Verschlüsselung - Verschlüsselung mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18008	FM ePA: putDocuments - Verschlüsselung der Dokumente mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18009	FM ePA: getDocuments - Entschlüsselung der Dokumente mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18182-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - wiederholte PIN-Eingabe	gemSpec_FM_ePA
A_20510	FM ePA: Autorisierung Aktensession - Fehler - Key Locked	gemSpec_FM_ePA
A_20571	FM ePA: PHRManagementService - Berechtigung in Komponente Autorisierung - Fehler - Key Locked	gemSpec_FM_ePA
A_20615	FM ePA: Dokumentenverwaltung - TLS Session Resumption mittels Session-ID nutzen	gemSpec_FM_ePA
A_20711	FM ePA: PHR_Service: Weiterleiten einer removeMetadata-Anfrage	gemSpec_FM_ePA
A_20712	FM ePA: PHR_Service: Weiterleiten von removeMetadata-Antwort	gemSpec_FM_ePA
A_21148	FM ePA: PHRService - HomeCommunityId verpflichtend	gemSpec_FM_ePA
A_21814	FM ePA: Autorisierung Aktensession - Fehler - AUTHORIZATION_ERROR	gemSpec_FM_ePA
A_22445	FM ePA: PHRManagementService - Authentisierung mittels SM-B	gemSpec_FM_ePA
A_22446	FM ePA: GetAuthorizationState - Abfrage der Berechtigungen einer Akte	gemSpec_FM_ePA
A_22460-01	FM ePA: GetAuthorizationState - Rückgabe der Berechtigungen einer Akte	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_22462	GetAuthorizationList - Beschränkung der Häufigkeit der Abfrage berechtigter Aktenkonten durch Konnektor - Fehler	gemSpec_FM_ePA
A_22463	GetAuthorizationState - Häufigkeit der Abfrage von Berechtigungen - Fehler	gemSpec_FM_ePA
A_22498	Konfiguration in RU und TU	gemSpec_FM_ePA
A_22703-01	FM ePA: RequestFacilityAuthorization Version 2.5 - Anzeige am Kartenterminal - Anzeigetext	gemSpec_FM_ePA
A_22785	FM ePA: GetAuthorizationState - Abweichung zur Definition von UserAgent	gemSpec_FM_ePA
A_23143	FM ePA: Fachmodulprotokoll (Fehler) - Fehler von Fachdiensten und zentralen Diensten	gemSpec_FM_ePA
A_23147	FM ePA: PHRManagementService Version 2.5.2	gemSpec_FM_ePA
A_23153	FM ePA: RequestFacilityAuthorization - Berechtigungen in Dokumentenverwaltung einbringen - Fehler bei gesetzlichen Vorgaben	gemSpec_FM_ePA
A_23516	FM ePA: PHRService Version 2.0.2	gemSpec_FM_ePA
A_23517	FM ePA: PHRManagementService Version 2.5.3	gemSpec_FM_ePA
A_23706	FM ePA: PHRManagementService Version 2.0.2	gemSpec_FM_ePA
NFDM-A_2333	Technisches Informationsmodell notfallrelevante medizinische Informationen (XSD)	gemSpec_InfoNFDM
NFDM-A_2334	Technisches Informationsmodell persönliche Erklärungen des Versicherten (XSD)	gemSpec_InfoNFDM
NFDM-A_2381	Technisches Informationsmodell Relevanz "Validitätskriterium"	gemSpec_InfoNFDM
AMTS-A_2227	FM AMTS: Info-Modell – Umsetzung des XML-Schemas der Einwilligungsdaten	gemSpec_Info_AMTS
AMTS-A_2228	FM AMTS: Info-Modell – Umsetzung des XML-Schemas der eMP/AMTS-Daten	gemSpec_Info_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2229	FM AMTS: Info-Modell – Beibehaltung der Reihenfolge in den eMP/AMTS-Daten	gemSpec_Info_AMTS
AMTS-A_2634	FM AMTS: Info-Modell – Annotations im XML-Schema der Einwilligungsdaten	gemSpec_Info_AMTS
AMTS-A_2635	FM AMTS: Info-Modell – Annotations im XML-Schema der eMP/AMTS-Daten	gemSpec_Info_AMTS
AMTS-A_2636	FM AMTS: Info-Modell – Validierung des Zeichensatz	gemSpec_Info_AMTS
TIP1-A_6103	SOAP-Version	gemSpec_KSR
A_22869	K_externeWelt, SICCT PERFORM VERIFICATION, lokale PIN-Eingabe	gemSpec_KT
A_22871	K_externeWelt: SICCT PERFORM VERIFICATION, remote PIN-Eingabe	gemSpec_KT
A_14159	Rückgabe von Fehlermeldungen an der Außenschnittstelle	gemSpec_Kon
A_15601	SOAP für Web-Services der Basisdienste	gemSpec_Kon
A_15606	Character Encoding für Web-Services	gemSpec_Kon
A_15607	SOAP für Web-Services der Fachmodule	gemSpec_Kon
A_15608	Web-Services der Fachmodule konform zu [BasicProfile1.2]	gemSpec_Kon
A_15609	Web-Services der Fachmodule konform zu [BasicProfile2.0]	gemSpec_Kon
A_15610	Verwendung von MTOM für Antwortnachricht	gemSpec_Kon
A_15611	SOAP Message Transmission Optimization Mechanism für Fachmodule	gemSpec_Kon
A_15786	SOAP Message Transmission Optimization Mechanism für Basisdienste - Einschränkung	gemSpec_Kon
A_17225-01	Aufbau einer sicheren Verbindung zur Vertrauenswürdige Ausführungsumgebung (VAU)	gemSpec_Kon
A_17295-01	Verwendung der intendedKeyUsage bei der Zertifikatsprüfung (ECC-Migration)	gemSpec_Kon
A_17473	TUC_KON_058 „Displaygröße ermitteln“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_17572	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_Kon
A_17661	Gesicherte Übertragung der Hash-Datei für TSL (ECC-Migration)	gemSpec_Kon
A_17746	Einsatzbereich und Vorgaben für Ver- und Entschlüsselung (ECC-Migration)	gemSpec_Kon
A_17768	Zertifikate und Schlüssel für Signaturerstellung und Signaturprüfung (QES und nonQES)	gemSpec_Kon
A_17781	Aktualisierung der TSL ohne Hash-Datei für TSL (ECC-Migration)	gemSpec_Kon
A_18389	Nur Nutzung von zugelassenen Versionen	gemSpec_Kon
A_18391	Automatisches Updates nicht nachholen	gemSpec_Kon
A_18686-01	Komfortsignatur-Timer	gemSpec_Kon
A_18780	PDF/A-3 DARF NICHT unterstützt werden	gemSpec_Kon
A_19052-01	Mindestanforderungen an Dokumente und Nachrichten	gemSpec_Kon
A_19100-01	Komfortsignatur-Zähler	gemSpec_Kon
A_19102-04	TUC_KON_158 „Komfortsignaturen erstellen“	gemSpec_Kon
A_19103-07	TUC_KON_170 "Dokumente mit Komfort signieren"	gemSpec_Kon
A_19104-04	TUC_KON_171 „Komfortsignatur einschalten“	gemSpec_Kon
A_19105	TUC_KON_172 „Komfortsignatur ausschalten“	gemSpec_Kon
A_19106-02	TUC_KON_173 „Liefere Signaturmodus“	gemSpec_Kon
A_19107	Operation ActivateComfortSignature	gemSpec_Kon
A_19108	Operation DeactivateComfortSignature	gemSpec_Kon
A_19109-02	Operation GetSignatureMode	gemSpec_Kon
A_19738	Optionaler Import von Konfigurationsdaten durch lokalen Administrator	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_19945	Unterstützte Signaturvarianten bei Komfortsignatur	gemSpec_Kon
A_20073-01	Prüfung der Länge der UserId	gemSpec_Kon
A_20074	UserId über 1.000 Vorgänge eindeutig	gemSpec_Kon
A_20536	TSL im kritischen Betriebszustand	gemSpec_Kon
A_20748	Automatischer TSL Download im kritischen Zustand	gemSpec_Kon
A_21137	Konnektor:Betriebsdaten - Formatierung der Betriebsdaten	gemSpec_Kon
A_21140	Konnektor:Betriebsdaten - Keine personenbezogenen und medizinischen Daten senden	gemSpec_Kon
A_21158	Mindestanzahl von CV-Crosszertifikaten	gemSpec_Kon
A_21224-01	Authentifizierung für Verbindungen zwischen Konnektor und Clientsystemen bei LDAP	gemSpec_Kon
A_21225	Konnektor:Betriebsdaten - Annotations im XML-Schema	gemSpec_Kon
A_21697-01	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	gemSpec_Kon
A_21698	Importiertes Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon
A_21699-02	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
A_21701	X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen exportieren	gemSpec_Kon
A_21702	Intern generierte Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_21760-01	ID.AK.AUT auf gSMC-K für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon
A_21811-03	Vorgaben für generierte und importierte Schlüssel und Zertifikate	gemSpec_Kon
A_21899	Kein Restart des Konnektors nach Aktualisierung der Bestandsnetze.xml	gemSpec_Kon
A_22344	Mindestens zwei parallele Komfortsignatursessions für einen HBA	gemSpec_Kon
A_22352	Unabhängige Komfortsignatur-Timer bei parallelen Komfortsignatursessions	gemSpec_Kon
A_22459	Unabhängige Komfortsignatur-Zähler bei parallelen Komfortsignatursessions	gemSpec_Kon
A_22673	Unerlaubte Inhalte in Dokumenten und Nachrichten	gemSpec_Kon
A_22970	Bedingung für den Betriebszustand EC_NK_Certificate_Expiring	gemSpec_Kon
A_23149	Konfigurationsschalter für Verwendung von ECC bei TLS (ECC-Migration)	gemSpec_Kon
A_23311	HBA Prüfung bei Steckvorgang	gemSpec_Kon
A_23536	TUC_KON_159 - "Signaturdatenelemente nachbereiten"	gemSpec_Kon
A_23545	Anzeige von Telematik-ID bei Auswahl der SMC-B	gemSpec_Kon
A_23546	Warnung bei unterschiedlichen Telematik-ID in einem Mandanten	gemSpec_Kon
A_23549	Unterstützung der importierten TI-Zertifikate	gemSpec_Kon
A_23614	SMC-B Prüfung bei Steckvorgang	gemSpec_Kon
A_23702	Keine Verzögerungen durch Prüfungen bei Steckvorgang	gemSpec_Kon
TIP1-A_4500-02	Dokumentgrößen von 25 MB	gemSpec_Kon
TIP1-A_4502	Zeichensatzcodierungen UTF-8 und ISO-8859-15	gemSpec_Kon
TIP1-A_4508	Konnektorzustand nach Bootup	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4509	Betriebszustand erfassen	gemSpec_Kon
TIP1-A_4510-05	Sicherheitskritische Fehlerzustände	gemSpec_Kon
TIP1-A_4512-05	Ereignis bei Änderung des Betriebszustandes	gemSpec_Kon
TIP1-A_4513	Betriebszustände anzeigen und Fehlerzustände zurücksetzen	gemSpec_Kon
TIP1-A_4514	Verfügbarkeit einer TLS-Schnittstelle	gemSpec_Kon
TIP1-A_4515	Verpflichtung zur Nutzung der TLS-Verbindung	gemSpec_Kon
TIP1-A_4516	Authentifizierung der Clients über Basic-Auth und X.509-Zertifikate	gemSpec_Kon
TIP1-A_4517-02	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4518-02	Konfiguration der Anbindung Clientsysteme	gemSpec_Kon
TIP1-A_4519-01	ab PTV4: Web-Services konform zu [BasicProfile1.2]	gemSpec_Kon
TIP1-A_4521	Protokollierung von Fehlern inkl. Trace-Struktur	gemSpec_Kon
TIP1-A_4522	Zugriffsberechtigungs-Informationsmodell des Konnektors	gemSpec_Kon
TIP1-A_4523	Sicherung der Aktualität des Informationsmodells Zugriffsberechtigungsdienst	gemSpec_Kon
TIP1-A_4524-03	TUC_KON_000 „Prüfe Zugriffsberechtigung“	gemSpec_Kon
TIP1-A_4525	Initialisierung Zugriffsberechtigungsdienst	gemSpec_Kon
TIP1-A_4526	Bearbeitung Informationsmodell Zugriffsberechtigungsdienst	gemSpec_Kon
TIP1-A_4527-04	TUC_KON_080 „Dokument validieren“	gemSpec_Kon
TIP1-A_4528	Bereitstellen des Dienstverzeichnisdienst	gemSpec_Kon
TIP1-A_4529-02	Formatierung der Ausgabedatei	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4532	Schnittstelle der Basisanwendung Dienstverzeichnisdienst	gemSpec_Kon
TIP1-A_4533	Dienstverzeichnisdienst initialisieren.	gemSpec_Kon
TIP1-A_4534	Kartenterminals nach eHealth-KT- Spezifikation	gemSpec_Kon
TIP1-A_4536	TLS-Verbindung zu Kartenterminals halten	gemSpec_Kon
TIP1-A_4537	KT-Statusanpassung bei Beendigung oder Timeout einer Netzwerkverbindung	gemSpec_Kon
TIP1-A_4538-02	ab PTV4: Wiederholter Verbindungsversuch zu den KTs	gemSpec_Kon
TIP1-A_4539	Robuster Kartenterminaldienst	gemSpec_Kon
TIP1-A_4540	Reaktion auf Dienstbeschreibungspakete	gemSpec_Kon
TIP1-A_4541	Reaktion auf KT-Slot-Ereignis – Karte eingesteckt	gemSpec_Kon
TIP1-A_4542	Reaktion auf KT-Slot-Ereignis – Karte entfernt	gemSpec_Kon
TIP1-A_4543	KT-Statusanpassung bei Beginn eines Updatevorgangs	gemSpec_Kon
TIP1-A_4544	KT-Statusanpassung bei Ende eines Updatevorgangs	gemSpec_Kon
TIP1-A_4545-03	TUC_KON_050 „Beginne Kartenterminalsitzung“	gemSpec_Kon
TIP1-A_4546	TUC_KON_054 „Kartenterminal hinzufügen“	gemSpec_Kon
TIP1-A_4547	TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	gemSpec_Kon
TIP1-A_4548-02	TUC_KON_053 „Paire Kartenterminal“	gemSpec_Kon
TIP1-A_4549	Initialisierung Kartenterminaldienst	gemSpec_Kon
TIP1-A_4550	Konfigurationsparameter des Kartenterminaldienstes	gemSpec_Kon
TIP1-A_4551	Einsichtnahme von Kartenterminaleinträgen	gemSpec_Kon
TIP1-A_4552	Manueller Verbindungsversuch zu Kartenterminals	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4553	Einsichtnahme in und Aktualisierung der Kartenterminaleinträge	gemSpec_Kon
TIP1-A_4554	Bearbeitung von Kartenterminaleinträgen	gemSpec_Kon
TIP1-A_4555	Manuelles Hinzufügen eines Kartenterminals	gemSpec_Kon
TIP1-A_4556	Pairing mit Kartenterminal durchführen	gemSpec_Kon
TIP1-A_4557	Ändern der Korrelationswerte eines Kartenterminals	gemSpec_Kon
TIP1-A_4560	Rahmenbedingungen für Kartensitzungen	gemSpec_Kon
TIP1-A_4561-02	Terminal-Anzeigen für PIN-Operationen	gemSpec_Kon
TIP1-A_4562	Reaktion auf „Karte entfernt“	gemSpec_Kon
TIP1-A_4563	Reaktion auf „Karte gesteckt“	gemSpec_Kon
TIP1-A_4565	TUC_KON_001 „Karte öffnen“	gemSpec_Kon
TIP1-A_4566	TUC_KON_026 „Liefere CardSession“	gemSpec_Kon
TIP1-A_4567	TUC_KON_012 „PIN verifizieren“	gemSpec_Kon
TIP1-A_4568	TUC_KON_019 „PIN ändern“	gemSpec_Kon
TIP1-A_4569-02	TUC_KON_021 „PIN entsperren“	gemSpec_Kon
TIP1-A_4570	TUC_KON_022 „Liefere PIN-Status“	gemSpec_Kon
TIP1-A_4572	TUC_KON_005 „Card-to-Card authentisieren“	gemSpec_Kon
TIP1-A_4573	TUC_KON_202 „LeseDatei“	gemSpec_Kon
TIP1-A_4574	TUC_KON_203 „SchreibeDatei„	gemSpec_Kon
TIP1-A_4577	TUC_KON_214 „FügeHinzRecord“	gemSpec_Kon
TIP1-A_4579	TUC_KON_018 „eGK-Sperrung prüfen“	gemSpec_Kon
TIP1-A_4580	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	gemSpec_Kon
TIP1-A_4581	TUC_KON_218 „Signiere“	gemSpec_Kon
TIP1-A_4582	TUC_KON_219 „Entschlüssele“	gemSpec_Kon
TIP1-A_4583	TUC_KON_200 „SendeAPDU“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4584	TUC_KON_024 „Karte zurücksetzen“	gemSpec_Kon
TIP1-A_4585	TUC_KON_216 „LeseZertifikat“	gemSpec_Kon
TIP1-A_4586-03	Basisanwendung Kartendienst	gemSpec_Kon
TIP1-A_4587	Operation VerifyPin	gemSpec_Kon
TIP1-A_4588	Operation ChangePin	gemSpec_Kon
TIP1-A_4589	Operation GetPinStatus	gemSpec_Kon
TIP1-A_4590	Operation UnblockPin	gemSpec_Kon
TIP1-A_4592	Konfigurationswerte des Kartendienstes	gemSpec_Kon
TIP1-A_4593	TUC_KON_025 „Initialisierung Kartendienst“	gemSpec_Kon
TIP1-A_4594	Richtung bei Verbindungsaufbau des Systeminformationsdienstes	gemSpec_Kon
TIP1-A_4595	Gesicherte Übertragung von Ereignissen	gemSpec_Kon
TIP1-A_4596	Nachrichtenaufbau und -kodierung des Systeminformationsdienstes	gemSpec_Kon
TIP1-A_4597	Unterstützung von Missbrauchserkennungen	gemSpec_Kon
TIP1-A_4598-02	TUC_KON_256 „Systemereignis absetzen“	gemSpec_Kon
TIP1-A_4599	TUC_KON_252 „Liefere KT_Liste“	gemSpec_Kon
TIP1-A_4600	TUC_KON_253 „Liefere Karten_Liste“	gemSpec_Kon
TIP1-A_4602	TUC_KON_254 „Liefere Ressourcendetails“	gemSpec_Kon
TIP1-A_4603-02	Basisanwendung Systeminformationsdienst	gemSpec_Kon
TIP1-A_4604	Operation GetCardTerminals	gemSpec_Kon
TIP1-A_4605	Operation GetCards	gemSpec_Kon
TIP1-A_4607	Operation GetResourceInformation	gemSpec_Kon
TIP1-A_4608	Operation Subscribe	gemSpec_Kon
TIP1-A_4609	Operation Unsubscribe	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4610	Operation GetSubscription	gemSpec_Kon
TIP1-A_4611	Konfigurationswerte des Systeminformationsdienstes	gemSpec_Kon
TIP1-A_4612	Maximale Anzahl an Subscriptions	gemSpec_Kon
TIP1-A_4613	Initialisierung Subscriptions-Liste beim Bootup	gemSpec_Kon
TIP1-A_4614	Missbrauchserkennung Verschlüsselungsdienst	gemSpec_Kon
TIP1-A_4616-03	TUC_KON_070 „Daten hybrid verschlüsseln“	gemSpec_Kon
TIP1-A_4617-02	TUC_KON_071 „Daten hybrid entschlüsseln“	gemSpec_Kon
TIP1-A_4620-03	Basisdienst Verschlüsselungsdienst	gemSpec_Kon
TIP1-A_4621-05	Operation EncryptDocument	gemSpec_Kon
TIP1-A_4622-05	Operation DecryptDocument	gemSpec_Kon
TIP1-A_4623-02	Unterstützte Signaturverfahren nonQES	gemSpec_Kon
TIP1-A_4624	Default-Signaturverfahren nonQES	gemSpec_Kon
TIP1-A_4627	Unterstützte Signaturverfahren QES	gemSpec_Kon
TIP1-A_4628	Default-Signaturverfahren QES	gemSpec_Kon
TIP1-A_4629	Unterstützte Karten QES-Erstellung	gemSpec_Kon
TIP1-A_4639	Generierung von Jobnummern für PIN-Eingaben	gemSpec_Kon
TIP1-A_4640	Anzeige der Jobnummern für PIN-Eingaben	gemSpec_Kon
TIP1-A_4643	Beschaffenheit der Jobnummer	gemSpec_Kon
TIP1-A_4645	Zeichen der Jobnummer	gemSpec_Kon
TIP1-A_4646-06	TUC_KON_155 „Dokumente zur Signatur vorbereiten“	gemSpec_Kon
TIP1-A_4647-03	TUC_KON 165 „Signaturvoraussetzungen für nonQES prüfen“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4648	TUC_KON_166 „nonQES Signaturen erstellen“	gemSpec_Kon
TIP1-A_4649-02	TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	gemSpec_Kon
TIP1-A_4651-02	TUC_KON_154 „QES Signaturen erstellen“	gemSpec_Kon
TIP1-A_4653-03	TUC_KON_160 „Dokumente nonQES signieren“	gemSpec_Kon
TIP1-A_4654-05	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	gemSpec_Kon
TIP1-A_4655-03	TUC_KON_150 „Dokument QES signieren“	gemSpec_Kon
TIP1-A_4669	QES-Stapelsignatur	gemSpec_Kon
TIP1-A_4671	Verhalten des Konnektors beim Abbruch einer Stapelsignatur	gemSpec_Kon
TIP1-A_4672-05	TUC_KON_151 „QES-Dokumentensignatur prüfen“	gemSpec_Kon
TIP1-A_4676-09	Basisdienst Signatordienst (nonQES und QES)	gemSpec_Kon
TIP1-A_4682	Sicheres Einbringen des TI-Vertrauensankers	gemSpec_Kon
TIP1-A_4685	Vermeidung von Spitzenlasten bei TSL- und CRL-Download	gemSpec_Kon
TIP1-A_4686	Warnung vor und bei Ablauf der TSL	gemSpec_Kon
TIP1-A_4687	Warnung vor und bei Ablauf des TI-Vertrauensankers	gemSpec_Kon
TIP1-A_4689	Caching von OCSP-Antworten	gemSpec_Kon
TIP1-A_4690	Timeout und Graceperiod für OCSP-Anfragen	gemSpec_Kon
TIP1-A_4691	Ablauf der gSMC-K und der gesteckten Karten regelmäßig prüfen	gemSpec_Kon
TIP1-A_4692	Missbrauchserkennung, zu kontrollierende Operationen	gemSpec_Kon
TIP1-A_4695	TUC_KON_033 „Zertifikatsablauf prüfen“	gemSpec_Kon
TIP1-A_4696-03	TUC_KON_037 „Zertifikat prüfen“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4697	TUC_KON_034 „Zertifikatsinformationen extrahieren“	gemSpec_Kon
TIP1-A_4698-03	Basisanwendung Zertifikatsdienst	gemSpec_Kon
TIP1-A_4699-04	Operation CheckCertificateExpiration	gemSpec_Kon
TIP1-A_4700	Operation ReadCardCertificate	gemSpec_Kon
TIP1-A_4702-04	Konfigurierbarkeit des Zertifikatsdienstes	gemSpec_Kon
TIP1-A_4703-02	Vertrauensraumstatus anzeigen	gemSpec_Kon
TIP1-A_4704	Zertifikatsablauf anzeigen	gemSpec_Kon
TIP1-A_4705	TSL manuell importieren	gemSpec_Kon
TIP1-A_4708	Protokollierungsfunktion	gemSpec_Kon
TIP1-A_4712	Protokollierung erfolgreicher Kryptooperationen	gemSpec_Kon
TIP1-A_4713	Herstellerspezifische Systemprotokollierung	gemSpec_Kon
TIP1-A_4714	Art der Protokollierung	gemSpec_Kon
TIP1-A_4715	TUC_KON_271 „Schreibe Protokolleintrag“	gemSpec_Kon
TIP1-A_4716	Einsichtnahme und Veränderung der Protokolle	gemSpec_Kon
TIP1-A_4717	Konfigurationswerte des Protokollierungsdienstes	gemSpec_Kon
TIP1-A_4718	TUC_KON_272 „Initialisierung Protokollierungsdienst“	gemSpec_Kon
TIP1-A_4719	TLS-Dienst reagiert auf Veränderung LU_ONLINE	gemSpec_Kon
TIP1-A_4720-02	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	gemSpec_Kon
TIP1-A_4721	TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	gemSpec_Kon
TIP1-A_4722	TLS-Dienst initialisieren	gemSpec_Kon
TIP1-A_4723	Verhalten als IPv4 Router	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4729	Es darf kein dynamisches Routing verwendet werden	gemSpec_Kon
TIP1-A_4742	Kommunikation mit den Fachmodulen	gemSpec_Kon
TIP1-A_4759	Konfiguration LAN-Interface	gemSpec_Kon
TIP1-A_4788	Verhalten bei Abweichung zwischen lokaler Zeit und erhaltenen Zeit	gemSpec_Kon
TIP1-A_4789	Zustandsvariablen des Konnektor Zeitdiensts	gemSpec_Kon
TIP1-A_4791	Operation sync_Time	gemSpec_Kon
TIP1-A_4792	Explizites Anstoßen der Zeitsynchronisierung	gemSpec_Kon
TIP1-A_4794	Warnung und Übergang in kritischen Betriebszustand bei nichterfolgter Zeitsynchronisierung	gemSpec_Kon
TIP1-A_4796	Grundlagen des Namensdienstes	gemSpec_Kon
TIP1-A_4801-02	ab PTV4: TUC_KON_361 „DNS-Namen auflösen“	gemSpec_Kon
TIP1-A_4804	Basisanwendung Namensdienst	gemSpec_Kon
TIP1-A_4806-01	Verpflichtende Managementschnittstelle	gemSpec_Kon
TIP1-A_4808-01	Zugangsschutz der Managementschnittstelle	gemSpec_Kon
TIP1-A_4812	Anzeige der Versionsinformationen (Selbstauskunft)	gemSpec_Kon
TIP1-A_4813	Persistieren der Konfigurationsdaten	gemSpec_Kon
TIP1-A_4818	Konfigurieren von Fachmodulen	gemSpec_Kon
TIP1-A_4831	KT-Update nach Wiedererreichbarkeit erneut anstoßen	gemSpec_Kon
TIP1-A_4833-02	TUC_KON_281 „Kartenterminalaktualisierung anstoßen“	gemSpec_Kon
TIP1-A_4834	TUC_KON_282 „UpdateInformationen beziehen“	gemSpec_Kon
TIP1-A_4835-02	Konfigurationswerte des KSR-Client	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4836-02	ab PTV4: Automatische Prüfung und Download von Update-Paketen	gemSpec_Kon
TIP1-A_4837	Übersichtsseite des KSR-Client	gemSpec_Kon
TIP1-A_4838	Einsichtnahme in Update-Informationen	gemSpec_Kon
TIP1-A_4839-01	Festlegung der durchzuführenden Updates	gemSpec_Kon
TIP1-A_4840-01	Manuelles Auslösen der durchzuführenden Updates	gemSpec_Kon
TIP1-A_4982	Anzeige von TU/RU in der Managementschnittstelle	gemSpec_Kon
TIP1-A_4985	TUC_KON_055 „Befülle CT-Object“	gemSpec_Kon
TIP1-A_4986	Informationsparameter des Kartenterminaldienstes	gemSpec_Kon
TIP1-A_4988-02	Unterstützung von Kartengenerationen	gemSpec_Kon
TIP1-A_5005	Protokollierung in der Managementschnittstelle	gemSpec_Kon
TIP1-A_5009	Authentifizierungsvarianten für Verbindungen zwischen Konnektor und Clientsystemen	gemSpec_Kon
TIP1-A_5010-10	Operation SignDocument (nonQES und QES)	gemSpec_Kon
TIP1-A_5011	Import von Kartenterminal-Informationen	gemSpec_Kon
TIP1-A_5012	Remote-PIN-Verfahren	gemSpec_Kon
TIP1-A_5033	Missbrauchserkennung Signatordienst (nonQES)	gemSpec_Kon
TIP1-A_5034-06	Operation VerifyDocument (nonQES und QES)	gemSpec_Kon
TIP1-A_5035	Operation GetIPAddress	gemSpec_Kon
TIP1-A_5058-01	ab PTV4: Fehlerübermittlung durch gematik-SOAP-Fault	gemSpec_Kon
TIP1-A_5110-02	Übersicht über alle verfügbaren Karten	gemSpec_Kon
TIP1-A_5111	PIN-Management der SM-Bs für den Administrator	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_5112	Operation RenewSubscriptions	gemSpec_Kon
TIP1-A_5149-01	ExternalAuthenticate nur für Authentisierung mit HBAX und SM-B nutzen	gemSpec_Kon
TIP1-A_5401	Parallele Nutzbarkeit Clientsystemschnittstelle	gemSpec_Kon
TIP1-A_5402	Baseline-Profilierung der AdES-EPES-Profile	gemSpec_Kon
TIP1-A_5403	Common PKI konforme Profile	gemSpec_Kon
TIP1-A_5408	Terminal-Anzeigen beim Anfordern und Auswerfen von Karten	gemSpec_Kon
TIP1-A_5409	TUC_KON_056 „Karte anfordern“	gemSpec_Kon
TIP1-A_5410	TUC_KON_057 „Karte auswerfen“	gemSpec_Kon
TIP1-A_5411-02	Basisdienst Kartenterminaldienst	gemSpec_Kon
TIP1-A_5412	Operation RequestCard	gemSpec_Kon
TIP1-A_5413	Operation EjectCard	gemSpec_Kon
TIP1-A_5416	Initialisierung „Namensdienst und Dienstlokalisierung“	gemSpec_Kon
TIP1-A_5433	Manuell importierte X.509-CA-Zertifikate nur für hybride Verschlüsselung	gemSpec_Kon
TIP1-A_5434	Verschlüsselung/Entschlüsselung eines XML Dokuments ergibt unverändertes XML-Dokument	gemSpec_Kon
TIP1-A_5436	XML Dokument nach Entfernen der Signatur unverändert	gemSpec_Kon
TIP1-A_5437-02	Signaturverfahren für externe Authentisierung	gemSpec_Kon
TIP1-A_5439	Operation ExternalAuthenticate	gemSpec_Kon
TIP1-A_5447	Einsatzbereich der Signaturvarianten	gemSpec_Kon
TIP1-A_5449	Operation VerifyCertificate	gemSpec_Kon
TIP1-A_5476	TUC_KON_204 „LöscheDateiInhalt“	gemSpec_Kon
TIP1-A_5478	TUC_KON_036 „LiefereFachlicheRolle“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_5482-01	TUC_KON_042 „CV-Zertifikat prüfen“	gemSpec_Kon
TIP1-A_5486	TUC_KON_027 „PIN-Schutz ein-/ausschalten“	gemSpec_Kon
TIP1-A_5487	Operation EnablePin	gemSpec_Kon
TIP1-A_5488	Operation DisablePin	gemSpec_Kon
TIP1-A_5505	TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“	gemSpec_Kon
TIP1-A_5517-02	Konnektor, TUC_KON_290 „LDAP-Verbindung aufbauen“	gemSpec_Kon
TIP1-A_5518	Konnektor, TUC_KON_291 „Verzeichnis abfragen“	gemSpec_Kon
TIP1-A_5519	Konnektor, TUC_KON_292 „LDAP-Verbindung trennen“	gemSpec_Kon
TIP1-A_5520	Konnektor, TUC_KON_293 „Verzeichnisabfrage abbrechen“	gemSpec_Kon
TIP1-A_5521	Konnektor, LDAPv3 Operationen	gemSpec_Kon
TIP1-A_5530	Kommunikation mit NET_TI_OFFENE_FD	gemSpec_Kon
TIP1-A_5536	Connector Event Transport Protocol über TCP	gemSpec_Kon
TIP1-A_5538	Signaturrichtlinien bei QES für XML-Dokumentenformate	gemSpec_Kon
TIP1-A_5540-01	QES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt	gemSpec_Kon
TIP1-A_5541-01	Referenzen in Dokumenten nicht dynamisch auflösen	gemSpec_Kon
TIP1-A_5542	Konnektor, Funktion zur Prüfung der Erreichbarkeit von Systemen	gemSpec_Kon
TIP1-A_5543	Keine manuelle PIN-Eingabe für gSMC-K	gemSpec_Kon
TIP1-A_5545	nonQES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt	gemSpec_Kon
TIP1-A_5657-02	Freischaltung von Softwareupdates	gemSpec_Kon
TIP1-A_5662	Gesicherte Übertragung von BNetzA-VL und Hashwert	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_5663	Prüfung der technischen Rolle bei TLS-Verbindungsaufbau zum TSL-Dienst	gemSpec_Kon
TIP1-A_5664	Reihenfolge der Dokumente bei Stapelsignatur	gemSpec_Kon
TIP1-A_5665-03	Basisdienst Authentifizierungsdienst	gemSpec_Kon
TIP1-A_5666-02	Operation StopSignature (nonQES und QES)	gemSpec_Kon
TIP1-A_5667	Operation GetJobNumber	gemSpec_Kon
TIP1-A_5682	XML Nicht geeignete Algorithmen im VerificationReport	gemSpec_Kon
TIP1-A_5694-03	ab PTV5: SOAP Message Transmission Optimization Mechanism für Basisdienste	gemSpec_Kon
TIP1-A_5698	Löschen von Kartenterminaleinträgen	gemSpec_Kon
TIP1-A_5938	TUC_KON_284 „KSR-Client initialisieren“	gemSpec_Kon
TIP1-A_6031	Kein selbsttätiges Zurücksetzen der SM-B	gemSpec_Kon
TIP1-A_6477	Manuelles Service Discovery	gemSpec_Kon
TIP1-A_6478	Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein	gemSpec_Kon
TIP1-A_6725	Lebensdauer von Textanzeigen am Kartenterminal	gemSpec_Kon
TIP1-A_6728	BNetzA-VL manuell importieren	gemSpec_Kon
TIP1-A_6729	TUC_KON_031 „BNetzA-VL aktualisieren“	gemSpec_Kon
TIP1-A_6730	Regelmäßige Aktualisierung der BNetzA-VL	gemSpec_Kon
TIP1-A_6731	Regelmäßige Prüfung der BNetzA-VL	gemSpec_Kon
TIP1-A_6732	Vermeidung von Spitzenlasten bei BNetzA-VL-Download	gemSpec_Kon
TIP1-A_6733	Aktive BNetzA-VL anzeigen	gemSpec_Kon
TIP1-A_7220	Konnektoraktualisierung File Transfer Ranges	gemSpec_Kon
TIP1-A_7254	Reaktion auf OCSP-Abfrage beim TLS-Verbindungsaufbau	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_7255	Anzeige von Fachmodulversionen	gemSpec_Kon
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	gemSpec_Kon
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	gemSpec_Kon
TIP1-A_7279	Authentifizierung des Remote-Administrators	gemSpec_Kon
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	gemSpec_Kon
A_16897	VAU-Protokoll: Versand der VAUClientHello-Nachricht	gemSpec_Krypt
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17209	Signaturverfahren für externe Authentisierung (ECC-Migration)	gemSpec_Krypt
A_17359	Signaturen binärer Daten (Dokumente) (ECC-Migration)	gemSpec_Krypt
A_22342	Konnektor, IKE-Schlüsselaushandlung – Erleichterung Migrationsphase 1 (ECC-Migration)	gemSpec_Krypt
A_22457	TLS-Clients, Ciphersuiten bei TLS-Verbindung mit eHealth-KT	gemSpec_Krypt
A_22458	TLS-Algorithmus passend zum Pairing	gemSpec_Krypt
GS-A_5071-01	kryptographische Vorgaben für eine Signaturprüfung in der SAK-Konnektor	gemSpec_Krypt
GS-A_5080-01	Signaturen binärer Daten (Dokumente)	gemSpec_Krypt
GS-A_5081-01	Signaturen von PDF/A-Dokumenten	gemSpec_Krypt
GS-A_5091	Verwendung von RSASSA-PSS bei XMLDSig-Signaturen	gemSpec_Krypt
GS-A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
GS-A_5345-01	TLS-Verbindungen Konnektor	gemSpec_Krypt
GS-A_5525	TLS-Renegotiation Konnektor	gemSpec_Krypt
GS-A_3834	DNS-Protokoll, Nameserver-Implementierungen	gemSpec_Net

ID	Bezeichnung	Quelle (Referenz)
GS-A_3932	Abfrage der in der Topologie am nächsten stehenden Nameservers	gemSpec_Net
GS-A_3933	NTP-Server-Implementierungen, Protokoll NTPv4	gemSpec_Net
GS-A_3934	NTP-Client-Implementierungen, Protokoll NTPv4	gemSpec_Net
GS-A_3935	NTP-Server-Implementierungen, Kiss-o'-Death	gemSpec_Net
GS-A_3938	NTP-Server-Implementierungen, Association Mode und Polling Intervall	gemSpec_Net
GS-A_3945	NTP-Server-Implementierungen, SNTP	gemSpec_Net
GS-A_4053	Ingress und Egress Filtering	gemSpec_Net
GS-A_4069	Erlaubter Verkehr Produkttypen	gemSpec_Net
GS-A_4070	Netzwerksteuerungsprotokolle	gemSpec_Net
GS-A_4075	Produkttyp Konnektor, Maximale Abweichung der Zeitinformation des NTP-Servers	gemSpec_Net
GS-A_4811	Produkttyp Konnektor, DNS-SD, Interpretation von TXT Resource Records	gemSpec_Net
GS-A_4832	Path MTU Discovery und ICMP Response	gemSpec_Net
GS-A_4835-01	Festlegung der Dienstklassen zur Priorisierung	gemSpec_Net
GS-A_4849	Produkttyp Konnektor, recursive queries	gemSpec_Net
GS-A_4884	Erlaubte ICMP-Types	gemSpec_Net
A_15237	Transport Fehlermeldungen als gematik-SOAP-Fault- SOAP 1.2	gemSpec_OM
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3700	Versionierung von Produkten auf Basis von dezentralen Produkttypen der TI-Plattform durch die Produktidentifikation	gemSpec_OM
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS-A_3796	Transport Fehlermeldungen als gematik-SOAP-Fault - SOAP 1.1	gemSpec_OM

ID	Bezeichnung	Quelle (Referenz)
GS-A_3801	Abbildung von Fehlern auf Transportprotokollebene	gemSpec_OM
GS-A_3856-02	Struktur der Fehlermeldungen	gemSpec_OM
GS-A_4547	Generische Fehlermeldungen	gemSpec_OM
GS-A_4858	Nutzung von Herstellerspezifischen Errorcodes (Konnektor)	gemSpec_OM
GS-A_4867	Übernahme Firmware-Gruppe	gemSpec_OM
GS-A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe	gemSpec_OM
GS-A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version	gemSpec_OM
GS-A_4872	Kein Downgrade der Firmware-Gruppe	gemSpec_OM
GS-A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5034	Inhalte der Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
A_17700	TSL-Auswertung ServiceTypeIdentifizier "unspecified"	gemSpec_PKI
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4646	TUC_PKI_017: Lokalisierung TSL Download-Adressen	gemSpec_PKI
GS-A_4647	TUC_PKI_016: Download der TSL-Datei	gemSpec_PKI
GS-A_4648	TUC_PKI_019: Prüfung der Aktualität der TSL	gemSpec_PKI
GS-A_4649	TUC_PKI_020: XML-Dokument validieren	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	gemSpec_PKI
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	gemSpec_PKI
GS-A_4652-01	TUC_PKI_018: Zertifikatsprüfung in der TI	gemSpec_PKI
GS-A_4653-01	TUC_PKI_002: Gültigkeitsprüfung des Zertifikats	gemSpec_PKI
GS-A_4654-01	TUC_PKI_003: CA-Zertifikat finden	gemSpec_PKI
GS-A_4655-01	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	gemSpec_PKI
GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	gemSpec_PKI
GS-A_4657-03	TUC_PKI_006: OCSP-Abfrage	gemSpec_PKI
GS-A_4658	Zertifikatsprüfung in spezifizierten Offline-Szenarien	gemSpec_PKI
GS-A_4660-02	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS-A_4661-01	kritische Erweiterungen in Zertifikaten	gemSpec_PKI
GS-A_4662	Bedingungen für TLS-Handshake	gemSpec_PKI
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	gemSpec_PKI
GS-A_4749-01	TUC_PKI_007: Prüfung Zertifikatstyp	gemSpec_PKI
GS-A_4750-01	TUC_PKI_030 „QES-Zertifikatsprüfung“	gemSpec_PKI
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	gemSpec_PKI
GS-A_4829	TUCs, Fehlerbehandlung	gemSpec_PKI
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4957-01	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
GS-A_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	gemSpec_PKI
GS-A_5484	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	gemSpec_PKI
A_16174	Performance - Fachmodul ePA - Bearbeitungszeit für Login	gemSpec_Perf
A_17490	Performance - Fachmodul ePA - Bearbeitungszeit	gemSpec_Perf
A_17491	Performance - Fachmodul ePA - Parallele Verarbeitung	gemSpec_Perf
A_17803	Performance - Fachmodul ePA - Bedingungen für die Messung	gemSpec_Perf
GS-A_5097	Performance – Konnektor in LE-U3 – Bearbeitungszeit lastfrei	gemSpec_Perf
GS-A_5098	Performance – Konnektor in LE-U4 – Bearbeitungszeit lastfrei	gemSpec_Perf
GS-A_5100	Performance – Konnektor in LE-U3 – Parallele Verarbeitung VSDM	gemSpec_Perf
GS-A_5101	Performance – Konnektor in LE-U4 – Parallele Verarbeitung VSDM	gemSpec_Perf
GS-A_5103	Performance – Konnektor in LE-U3 – Parallele Verarbeitung	gemSpec_Perf
GS-A_5104	Performance – Konnektor in LE-U4 – Parallele Verarbeitung	gemSpec_Perf
GS-A_5108	Performance – Konnektor in LE-U3 – Verfügbarkeit	gemSpec_Perf
GS-A_5109	Performance – Konnektor in LE-U4 – Verfügbarkeit	gemSpec_Perf
GS-A_5130	Performance – Konnektor – Performance Logging	gemSpec_Perf
GS-A_5247	Performance – Konnektor – G2-Karten mit unterschiedlicher CV-Root	gemSpec_Perf
GS-A_5328	Performance – Konnektor – TLS-Handshake	gemSpec_Perf
GS-A_5332	Performance – Konnektor – Robustheit gegenüber Lastspitzen	gemSpec_Perf

ID	Bezeichnung	Quelle (Referenz)
GS-A_5333	Performance – Konnektor – TLS Session Resumption 1	gemSpec_Perf
GS-A_5334	Performance – Konnektor – TLS Session Resumption 2	gemSpec_Perf
GS-A_5487	Performance – Konnektor – Parallele Verarbeitung AMTS	gemSpec_Perf
A_17893	Maximale Größe der JSON-Requests und -Responses	gemSpec_SGD_ePA
A_17925	SGD-Client, Parallele Anfrage SGD1 und SGD2	gemSpec_SGD_ePA
VSDM-A_2282	Fachmodul VSDM: RequestHeader bei Aufruf GetUpdateFlags	gemSpec_SST_FD_VSDM
VSDM-A_2285	Fachmodul VSDM: optionale Updates nicht ausführen	gemSpec_SST_FD_VSDM
VSDM-A_2298	Fachmodul VSDM: Sessioninformation für GetNextCommandPackage übernehmen	gemSpec_SST_FD_VSDM
VSDM-A_2303	Fachmodul VSDM: Request-Header bei Aufruf PerformUpdates	gemSpec_SST_FD_VSDM
VSDM-A_2308	Fachmodul VSDM: Operation PerformUpdates aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2310	Fachmodul VSDM: Operation GetUpdateFlags aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2311	Fachmodul VSDM: Operation GetNextCommandPackage aufrufen	gemSpec_SST_FD_VSDM
VSDM-A_2318	Fachmodul VSDM: Kommando-APDUs unverändert durchreichen	gemSpec_SST_FD_VSDM
VSDM-A_2321	Fachmodul VSDM: Request-Header bei Aufruf GetNextCommandPackage	gemSpec_SST_FD_VSDM
VSDM-A_2335	Fachmodul VSDM: AdditionalInfo nicht nutzen	gemSpec_SST_FD_VSDM
VSDM-A_2552	Fachmodul VSDM: Abbruch bei unerwarteten Statuscode	gemSpec_SST_FD_VSDM
VSDM-A_2553	Fachmodul VSDM: Response bei unerwarteten Statuscode	gemSpec_SST_FD_VSDM
VSDM-A_3008	Fachmodul VSDM: Response bei Abbruch	gemSpec_SST_FD_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2596	ReadVSD: Umsetzung des Anwendungsfalls "VSDM-UC_01: VSD von eGK lesen"	gemSpec_SST_PS_VSDM
VSDM-A_2608	ReadKVK: Umsetzung des Anwendungsfalls "VSDM-UC_03: Versichertendaten von KVK lesen"	gemSpec_SST_PS_VSDM
VSDM-A_2631	ReadVSD: ErrorCode im Prüfungsnachweis	gemSpec_SST_PS_VSDM
VSDM-A_2633	I_VSDService: Implementierung ReadVSD gemäß WSDL	gemSpec_SST_PS_VSDM
VSDM-A_2634	ReadVSD: Ausgangsparameter	gemSpec_SST_PS_VSDM
VSDM-A_2647	ReadVSD: GVD in Antwort optional	gemSpec_SST_PS_VSDM
VSDM-A_2658	Schnittstelle Primärsystem: BasicProfile 1.2	gemSpec_SST_PS_VSDM
VSDM-A_2675	Schnittstelle Primärsystem: invalide Anfragenachrichten erkennen	gemSpec_SST_PS_VSDM
VSDM-A_2676	Schnittstelle Primärsystem: zusätzliche Headerelemente	gemSpec_SST_PS_VSDM
VSDM-A_2677	I_KVKService: Implementierung ReadKVK gemäß WSDL	gemSpec_SST_PS_VSDM
VSDM-A_2678	Schnittstelle Primärsystem: Transportsicherung	gemSpec_SST_PS_VSDM
VSDM-A_2682	Fachmodul VSDM: Keine sicherheitsrelevanten Informationen im Fehlermeldungen	gemSpec_SST_PS_VSDM
VSDM-A_2689	Schnittstelle Primärsystem: auf zulässige Werte prüfen	gemSpec_SST_PS_VSDM
VSDM-A_2690	Fachmodul VSDM: Fehlercode bei nicht konsistenten VSD	gemSpec_SST_PS_VSDM
VSDM-A_2691	ReadVSD: Format der Ausgangsparameter	gemSpec_SST_PS_VSDM
VSDM-A_2692	Fachmodul VSDM: Lesen oder Dekomprimieren der VSD von der eGK scheitert	gemSpec_SST_PS_VSDM
VSDM-A_2693	ReadVSD: Eingangsparameter	gemSpec_SST_PS_VSDM
VSDM-A_2695	Fachmodul VSDM: Lesen der Daten von der KVK scheitert	gemSpec_SST_PS_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2696	Fachmodul VSDM: Prüfsumme des KVK-Satzes falsch	gemSpec_SST_PS_VSDM
VSDM-A_2703	Schnittstelle Primärsystem: nur erlaubte Header in Antwortnachricht	gemSpec_SST_PS_VSDM
VSDM-A_2710	ReadKVK: Eingangsparameter	gemSpec_SST_PS_VSDM
VSDM-A_2711	ReadKVK: Ausgangsparameter	gemSpec_SST_PS_VSDM
VSDM-A_2936	Fachmodul VSDM: Prüfungsnachweis nicht entschlüsselbar	gemSpec_SST_PS_VSDM
VSDM-A_2937	Fachmodul VSDM: Es ist kein Prüfungsnachweis auf der eGK vorhanden	gemSpec_SST_PS_VSDM
VSDM-A_2982	Fachmodul VSDM: Fehlermeldung: SM-B nicht freigeschaltet	gemSpec_SST_PS_VSDM
VSDM-A_2983	Fachmodul VSDM: Fehlermeldung: HBA nicht freigeschaltet	gemSpec_SST_PS_VSDM
VSDM-A_2189	Fachmodul VSDM: WS-I Basic Profile in der Version 1.2 umsetzen	gemSpec_SST_VSDM
VSDM-A_2190	Fachmodul VSDM: Nachrichten konform zu WSDL- und Schemadateien	gemSpec_SST_VSDM
VSDM-A_2194	Fachmodul VSDM: mit TLS-Client X.509-Zertifikat authentifizieren	gemSpec_SST_VSDM
VSDM-A_2199	Fachmodul VSDM: HTTP-Komprimierung nutzen	gemSpec_SST_VSDM
VSDM-A_2200	Fachmodul VSDM: HTTP-Komprimierung unterstützen	gemSpec_SST_VSDM
VSDM-A_2202	Fachmodul VSDM: nur spezifizierte Header-Elemente	gemSpec_SST_VSDM
VSDM-A_2203	Fachmodul VSDM: keine Whitespaces	gemSpec_SST_VSDM
VSDM-A_2204	Fachmodul VSDM: Antwortnachrichten validieren	gemSpec_SST_VSDM
VSDM-A_2205	Fachmodul VSDM: invalide Antwortnachrichten erkennen	gemSpec_SST_VSDM
VSDM-A_2206	Fachmodul VSDM: auf zulässige Werte validieren	gemSpec_SST_VSDM
VSDM-A_2207	Fachmodul VSDM: Toleranz gegenüber zusätzlichen Elementen	gemSpec_SST_VSDM

ID	Bezeichnung	Quelle (Referenz)
VSDM-A_2209	Fachmodul VSDM: Endpunkt-Adresse mit Lokalisierungsinformation bilden	gemSpec_SST_VSDM
VSDM-A_2211	Fachmodul VSDM: Lokalisierungsinformationen gemäß dem Schema bilden	gemSpec_SST_VSDM
VSDM-A_2212	Fachmodul VSDM: Sessionformationen gemäß Schema bilden	gemSpec_SST_VSDM
VSDM-A_2213	Fachmodul VSDM: SOAP Faults ohne gematik-Fehlerstruktur verarbeiten	gemSpec_SST_VSDM
VSDM-A_2214	Fachmodul VSDM: HTTP-Fehlermeldungen verarbeiten	gemSpec_SST_VSDM
VSDM-A_2215	Fachmodul VSDM: Header-Feld "Via" auswerten	gemSpec_SST_VSDM
VSDM-A_2216	Fachmodul VSDM: gematik SOAP Faults verarbeiten	gemSpec_SST_VSDM
VSDM-A_2217	Fachmodul VSDM: Nachrichten grundsätzlich nicht speichern	gemSpec_SST_VSDM
VSDM-A_2218	Fachmodul VSDM: Fehlermeldung speichern	gemSpec_SST_VSDM
VSDM-A_2219	Fachmodul VSDM: Anfragenachricht zu einer Fehlermeldung speichern	gemSpec_SST_VSDM
VSDM-A_2225	Fachmodul VSDM, Intermediär VSDM: TLS Session Resumption mittels Session-ID nutzen	gemSpec_SST_VSDM
VSDM-A_2226	Fachanwendung VSDM: Verbindung offen halten	gemSpec_SST_VSDM
VSDM-A_2235	Fachmodul VSDM: Trennzeichen in der URL	gemSpec_SST_VSDM
VSDM-A_2312	Fachmodul VSDM: Toleranz gegenüber nicht verarbeiteten Elementen	gemSpec_SST_VSDM
VSDM-A_2956	Fachmodul VSDM: generische Fehlermeldungen	gemSpec_SST_VSDM
VSDM-A_3003	Verschlüsselter Transport durch Fachmodul VSDM	gemSpec_SST_VSDM
GS-A_5502	Ausstellung im Format SAML 2.0	gemSpec_TBAuth
GS-A_5504	Geltende Präfixe und Namensräume	gemSpec_TBAuth

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_5120	Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen	gemSpec_TSL
TIP1-A_5566	LDAP Client, LDAPS	gemSpec_VZD
TIP1-A_5570	LDAP Client, TUC_VZD_0001 „search_Directory“	gemSpec_VZD
AMTS-A_2111	FM AMTS: WriteConsent – Fehlerbehandlung bei invaliden Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2114	FM AMTS: WriteConsent – Kein Überschreiben einer vorhandenen Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2115	FM AMTS: WriteConsent – Fehlermeldung bei vorhandenen Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2118	FM AMTS: ReadConsent – Fehlerbehandlung bei fehlenden Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2622	FM AMTS: Update des Timestamps in EF.StatusAMTS nach Schreibzugriff	gemSpec_eGK_Fach_AMTS
NFDM-A_2131	Speicherstruktur für EF.NFD	gemSpec_eGK_Fach_NFDM
NFDM-A_2132	Speicherstruktur EF.StatusNFD	gemSpec_eGK_Fach_NFDM
NFDM-A_2133	Speicherstruktur für EF.DPE	gemSpec_eGK_Fach_NFDM
NFDM-A_2134	Speicherstruktur EF.StatusDPE	gemSpec_eGK_Fach_NFDM
VSDM-A_2973	Speicherstruktur des Containers EF.PD auf eGK	gemSpec_eGK_Fach_VSDM
VSDM-A_2974	Speicherstruktur des Containers EF.VD auf eGK	gemSpec_eGK_Fach_VSDM
VSDM-A_2975	Speicherstruktur des Containers EF.GVD auf eGK	gemSpec_eGK_Fach_VSDM
VSDM-A_2976	Speicherstruktur des Containers EF.StatusVD auf der eGK	gemSpec_eGK_Fach_VSDM
TIP1-A_4701-02	TUC_KON_035 „Zertifikatsdienst initialisieren“	gemF_Highspeed-Konnektor
TIP1-A_4795-02	TUC_KON_352 „Initialisierung Zeitdienst“ (Highspeed-Konnektor)	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
A_14760-13	Nutzungsvorgaben für die Verwendung von XDS-Metadaten	gemSpec_DM_ePA
VSDM-A_3007	Fachmodul VSDM: Ermitteln der URL des zugeordneten VSDM-Intermediärs	gemSpec_FM_VSDM
A_13828-04	FM ePA: Service-Informationen für Dienstverzeichnisdienste	gemSpec_FM_ePA
A_14373-02	FM ePA: PHRService	gemSpec_FM_ePA
A_15142	FM ePA: Login—Ermittlung des Aufrufkontexts via SOAP-Header	gemSpec_FM_ePA
A_15142-01	FM ePA: Login—Ermittlung des Aufrufkontexts via SOAP-Header—PHRService Version 2.x	gemSpec_FM_ePA
A_15531-01	FM ePA: Dokumentenverwaltung—TLS-Verbindung zur Komponente Dokumentenverwaltung aufbauen	gemSpec_FM_ePA
A_15615-01	FM ePA: Übergreifende Anforderung—Ermittlung eines SM-B-Fehler	gemSpec_FM_ePA
A_16207	FM ePA: PHRService—Maximale Größe aller Dokumente	gemSpec_FM_ePA
A_16208	FM ePA: PHRService—Maximale Größe aller Dokumente—Fehler	gemSpec_FM_ePA
A_16209-01	FM ePA: PHRService—Maximale Größe eines Dokuments	gemSpec_FM_ePA
A_16210	FM ePA: PHRService—Maximale Größe eines Dokuments—Fehler	gemSpec_FM_ePA
A_16212-03	FM ePA: RequestFacilityAuthorization Version 1.x—Anzeige am Kartenterminal—Anzeigetext	gemSpec_FM_ePA
A_20090	Operation updateDocumentSet nicht unterstützt	gemSpec_FM_ePA
A_19103-06	TUC-KON-170 "Dokumente mit Komfort signieren"	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_21697	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	gemSpec_Kon
A_21699-01	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
A_21811-01	Vorgaben für generierte und importierte Schlüssel und Zertifikate entsprechend gemSpec_Krypt	gemSpec_Kon
A_23121	Konfigurationsschalter für Verwendung von ECC bei IPsec/IKE (ECC-Migration)	gemSpec_Kon
TIP1-A_4510-04	Sicherheitskritische Fehlerzustände	gemSpec_Kon
TIP1-A_4512-04	Ereignis bei Änderung des Betriebszustandes	gemSpec_Kon
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4646-04	ab PTV4: TUC_KON_155 „Dokumente zur Signatur vorbereiten“	gemSpec_Kon
TIP1-A_4647-02	TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“	gemSpec_Kon
TIP1-A_4649	TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	gemSpec_Kon
TIP1-A_4653-02	ab PTV4: TUC_KON_160 „Dokumente nonQES signieren“	gemSpec_Kon
TIP1-A_4654-04	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	gemSpec_Kon
TIP1-A_4655-02	TUC_KON_150 „Dokument QES signieren“	gemSpec_Kon
TIP1-A_4672-04	TUC_KON_151 „QES-Dokumentensignatur prüfen“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4676-08	Basisdienst-Signaturdienst (nonQES und QES)	gemSpec_Kon
TIP1-A_4688	OCSP-Forwarding	gemSpec_Kon
TIP1-A_4696-02	TUC_KON_037 „Zertifikat prüfen“	gemSpec_Kon
TIP1-A_4699-03	Operation-CheckCertificateExpiration	gemSpec_Kon
TIP1-A_4703-01	Vertrauensraumstatus-anzeigen	gemSpec_Kon
TIP1-A_4806	Verpflichtende Managementschnittstelle	gemSpec_Kon
TIP1-A_5010-09	Operation-SignDocument (nonQES und QES)	gemSpec_Kon
TIP1-A_5110	Übersicht über alle verfügbaren Karten	gemSpec_Kon

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_21884	Redundanter Aufbau Highspeed-Konnektor	gemF_Highspeed-Konnektor
A_21990	Kein Zugriff auf SM-B Identitäten und Kopplungs-Geheimnis durch Betreiber	gemF_Highspeed-Konnektor
A_22571	Benachrichtigung und Bereitstellung der Bestandsnetze.xml	gemF_Highspeed-Konnektor
A_22574	Zugang zum Highspeed Konnektor	gemF_Highspeed-Konnektor
A_22577	Highspeed-Konnektor: Bereitstellung TU-Anbindung	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
A_23475	Nachnutzung HSM durch TI-GW-Zugangsmodule	gemF_ TI Highspeed-GatKonnektor
A_23476	Zentrale Umsetzung von KSR-Client, NTP und Namensdienst	gemF_ TI Highspeed-GatKonnektor
A_23479	HSK, http-Forwarder - kein Cache	gemF_ TI Highspeed-GatKonnektor
A_23857	Highspeed-Konnektor: Betriebsdaten - Vermeiden von Spitzenlasten beim Senden von Betriebsdaten	gemF_Highspeed-Konnektor
A_15593	Ersatz bei defekten dezentralen Produkten	gemKPT_Test
A_15594	Vorhalten testbereiter dezentraler Komponenten	gemKPT_Test
A_20065	Nutzung der Dokumententemplates der gematik	gemKPT_Test
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2775	Performance in RU	gemKPT_Test
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemF KPT _HighspTeed-Konnektor
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6082	Versionen der Referenzobjekte	gemKPT_Test
TIP1-A_6086	Unterstützung bei Anbindung eines Produktes	gemKPT_Test
TIP1-A_6087	Zugang zur Adminschnittstelle bei dezentralen Produkten	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6517-01	Eigenverantwortlicher Test: TBI	gemKPT_Test

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524-01	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6527	Testkarten	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemFKPT_HighspTeed-Konnektor
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_7330	Tracedaten von echten Außenschnittstellen	gemFKPT_HighspTeed-Konnektor
TIP1-A_7331	Bereitstellung von Tracedaten an Außenschnittstelle	gemFKPT_HighspTeed-Konnektor
TIP1-A_7333	Parallelbetrieb von Release oder Produkttypversion	gemKPT_Test
TIP1-A_7334	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1-A_7358	Qualität des Produktmusters	gemKPT_Test
A_22464	Bezeichnung der Anwendung ePA	gemSpec_DM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_22470-01	Definition UserAgent	gemSpec_DM_ePA
AMTS-A_2133	FM AMTS: Allgemeine Fehlerbehandlung	gemSpec_FM_AMTS
AMTS-A_2141	FM AMTS: Einheitliches Protokollierungsformat	gemSpec_FM_AMTS
AMTS-A_2239	FM AMTS: Übergreifende Anforderung – Transaktionsstatus entfernen	gemSpec_FM_AMTS
NFDM-A_2095	Verbot Protokollierung medizinischer Daten	gemSpec_FM_NFDM
NFDM-A_2096	Verbot Protokollierung Schlüsselmaterial	gemSpec_FM_NFDM
NFDM-A_2097	Verbot Protokollierung personenbezogener Daten	gemSpec_FM_NFDM
NFDM-A_2098	Einheitliches Protokollierungsformat	gemSpec_FM_NFDM
NFDM-A_2105	Verbot der persistenten Speicherung medizinischer Daten	gemSpec_FM_NFDM
NFDM-A_2406	Protokollierung	gemSpec_FM_NFDM
VSDM-A_2635	Fachmodul VSDM: keine Protokollierung von medizinischen Daten	gemSpec_FM_VSDM
VSDM-A_2644	Fachmodul VSDM: Protokolldateien kopieren	gemSpec_FM_VSDM
VSDM-A_2649	Fachmodul VSDM: Protokolldateien begrenzen auf 180 Tage, Datenschutz	gemSpec_FM_VSDM
VSDM-A_2665	Fachmodul VSDM: Ereignisdienst - für Topics registrieren	gemSpec_FM_VSDM
VSDM-A_2874-01	Fachmodul VSDM: keine Protokollierung von personenbezogenen Daten	gemSpec_FM_VSDM
VSDM-A_3004	Fachmodul VSDM: Benutzerdokumentation: Verwendung unterschiedlicher Schlüssel VSDM-PNW-Key	gemSpec_FM_VSDM
A_14155	FM ePA: Verbot des Logging von medizinischen und personenbezogenen Daten	gemSpec_FM_ePA
A_14241	FM ePA: Übergreifende Anforderung - Unterstützte Generationen der eGK	gemSpec_FM_ePA
A_14354	FM ePA: Übergreifende Anforderung IHE - Keine Prüfung der Metadaten-Profilierung	gemSpec_FM_ePA
A_14374-03	FM ePA: Übergreifende Anforderung IHE - Profile, Akteure und Optionen	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_14376	FM ePA: PHRService - Fehlermeldungen gemäß IHE	gemSpec_FM_ePA
A_14710	FM ePA: Übergreifende Anforderung - Verwendung des Protokollierungsdienstes	gemSpec_FM_ePA
A_15143	FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (SM-B)	gemSpec_FM_ePA
A_15144	FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (eGK)	gemSpec_FM_ePA
A_15202	FM ePA: Authentisierung mit SM-B - Wiederverwendung der AuthenticationAssertion	gemSpec_FM_ePA
A_15203	FM ePA: Authentisierung mit SM-B - Löschen der AuthenticationAssertion	gemSpec_FM_ePA
A_15575	FM ePA: Übergreifende Anforderung - SOAP für Webservices	gemSpec_FM_ePA
A_16352	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - nicht darstellbare Zeichen von InsurantName und OrganizationName	gemSpec_FM_ePA
A_22462	GetAuthorizationList - Beschränkung der Häufigkeit der Abfrage berechtigter Aktenkonten durch Konnektor - Fehler	gemSpec_FM_ePA
NFDM-A_2333	Technisches Informationsmodell notfallrelevante medizinische Informationen (XSD)	gemSpec_InfoNFDM
NFDM-A_2334	Technisches Informationsmodell persönliche Erklärungen des Versicherten (XSD)	gemSpec_InfoNFDM
NFDM-A_2381	Technisches Informationsmodell Relevanz "Validitätskriterium"	gemSpec_InfoNFDM
AMTS-A_2230	FM AMTS: Info-Modell – Unterstützte Versionen bei Lesezugriffen	gemSpec_Info_AMTS
AMTS-A_2231	FM AMTS: Info-Modell – Unterstützte Version bei Schreibzugriffen	gemSpec_Info_AMTS
A_14159	Rückgabe von Fehlermeldungen an der Außenschnittstelle	gemSpec_Kon
A_15601	SOAP für Web-Services der Basisdienste	gemSpec_Kon
A_15607	SOAP für Web-Services der Fachmodule	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_15608	Web-Services der Fachmodule konform zu [BasicProfile1.2]	gemSpec_Kon
A_15609	Web-Services der Fachmodule konform zu [BasicProfile2.0]	gemSpec_Kon
A_15611	SOAP Message Transmission Optimization Mechanism für Fachmodule	gemSpec_Kon
A_15786	SOAP Message Transmission Optimization Mechanism für Basisdienste - Einschränkung	gemSpec_Kon
A_18597	Sicherheitszustand der PIN.QES bei Komfortsignatur	gemSpec_Kon
A_18756	Optionalität von nonQES-XAdES Signatur	gemSpec_Kon
A_18928	Ausstattung mit dual-personalisierten gSMC-K-X.509-Zertifikaten	gemSpec_Kon
A_18930	Unterstützung von gSMC-K Personalisierungsvarianten	gemSpec_Kon
A_19101	Handbuch-Hinweis zu Nutzerauthentisierung am Clientsystem bei Komfortsignatur	gemSpec_Kon
A_20531	Größe der Bestandsnetze.xml	gemSpec_Kon
A_21900	Minimale Anzahl von Reboots	gemSpec_Kon
A_22894-01	Handbuch Erläuterungen zur Zertifikatsauswahl	gemSpec_Kon
A_22971	Bedingung für den Betriebszustand EC_NK_Certificate_Expired	gemSpec_Kon
TIP1-A_4504	Keine Administratorinteraktion bei Einsatz mehrerer gSMC-Ks	gemSpec_Kon
TIP1-A_4506	Initiale Identitäten der gSMC-K	gemSpec_Kon
TIP1-A_4519-01	ab PTV4: Web-Services konform zu [BasicProfile1.2]	gemSpec_Kon
TIP1-A_4575	TUC_KON_209 „LeseRecord“	gemSpec_Kon
TIP1-A_4685	Vermeidung von Spitzenlasten bei TSL- und CRL-Download	gemSpec_Kon
TIP1-A_4710-02	Keine Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon
TIP1-A_4711	Kapazität der Protokolldateien	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4713	Herstellerspezifische Systemprotokollierung	gemSpec_Kon
TIP1-A_4790	TUC_KON_351 „Liefere Systemzeit“	gemSpec_Kon
TIP1-A_4798	DNS Stub-Resolver	gemSpec_Kon
TIP1-A_4802	TUC_KON_362 „Liste der Dienste abrufen“	gemSpec_Kon
TIP1-A_4803	TUC_KON_363 „Dienstdetails abrufen“	gemSpec_Kon
TIP1-A_4981	Steuerung der Betriebsumgebung via gSMC-K	gemSpec_Kon
TIP1-A_5387	Erweiterte Nutzung der AdES-Profile	gemSpec_Kon
TIP1-A_5536	Connector Event Transport Protocol über TCP	gemSpec_Kon
TIP1-A_5654	Sicherheits-Protokollierung	gemSpec_Kon
TIP1-A_5660	Hinweise im Handbuch für manuell importierte X.509-CA-Zertifikate	gemSpec_Kon
TIP1-A_5661	Automatisierung Managementschnittstelle	gemSpec_Kon
TIP1-A_5694-03	ab PTV5: SOAP Message Transmission Optimization Mechanism für Basisdienste	gemSpec_Kon
TIP1-A_5696	Prüfung der personalisierten gSMC-K	gemSpec_Kon
TIP1-A_6479	Keine Protokollierung vertraulicher Daten	gemSpec_Kon
A_15705	Vorgaben Aktenschlüssel (RecordKey) und Kontextschlüssel (ContextKey)	gemSpec_Krypt
A_16897	VAU-Protokoll: Versand der VAUClientHello-Nachricht	gemSpec_Krypt
A_16958	VAU-Protokoll: Client, Neuinitiiieren einer Schlüsselaushandlung	gemSpec_Krypt
A_17094-01	TLS-Verbindungen Konnektor (ECC-Migration)	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_18004	Vorgaben für die Kodierung von Chiffraten (innerhalb von ePA)	gemSpec_Krypt
A_18465-01	VAU-Protokoll: MTOM/XOP-HTTP-Header-Informationen	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_18466-01	VAU-Protokoll: zusätzliche HTTP-Header-Informationen	gemSpec_Krypt
A_20549	VAU-Protokoll: Einbringen der ursprünglich intendierten Content-Type-Variable	gemSpec_Krypt
A_23511	Konnektor, IOP, Kodierung ECC-Schlüssel, Primärsystem-Verbindungssicherung	gemSpec_Krypt
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4054	Paketfilter Default Deny	gemSpec_Net
GS-A_4831	Standards für IPv4	gemSpec_Net
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_3805	Loglevel zur Bezeichnung der Granularität FehlerLog	gemSpec_OM
GS-A_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM
GS-A_3807	Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
GS-A_3816	Festlegung sicherheitsrelevanter Fehler	gemSpec_OM
GS-A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM
GS-A_4875	Einschränkung der Firmware-Gruppe bei Verlust Zulassung	gemSpec_OM

ID	Bezeichnung	Quelle (Referenz)
GS-A_4876	Einschränkung der Firmware-Gruppe bei Verlust SigG-Bestätigung oder CC-Sicherheitszertifikat	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039-01	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
A_17803	Performance - Fachmodul ePA - Bedingungen für die Messung	gemSpec_Perf
GS-A_5036	Performance – Stapelsignatur Konnektor für LE-U3	gemSpec_Perf
GS-A_5106	Performance – Stapelsignatur Konnektor für LE-U4	gemSpec_Perf
A_18249	Groß- und Kleinschreibung von Daten in Hexadezimalform	gemSpec_SGD_ePA
A_18250	keine führenden Nullen bei Punktkoordinaten	gemSpec_SGD_ePA
A_18988	SGD-Client, Neustart des Protokolldurchlaufs	gemSpec_SGD_ePA
VSDM-A_2682	Fachmodul VSDM: Keine sicherheitsrelevanten Informationen im Fehlermeldungen	gemSpec_SST_PS_VSDM
VSDM-A_2208	Fachmodul VSDM: beliebige Reihenfolge der Header-Elemente	gemSpec_SST_VSDM
VSDM-A_2217	Fachmodul VSDM: Nachrichten grundsätzlich nicht speichern	gemSpec_SST_VSDM
VSDM-A_3066	Fachmodul VSDM: Kein Pipelining	gemSpec_SST_VSDM
TIP1-A_5568	VZD und LDAP Client, Implementierung der LDAPv3 search Operation	gemSpec_VZD
AMTS-A_2123	FM AMTS: Speicherstruktur EF.AMTS auf der eGK	gemSpec_eGK_Fach_AMTS
AMTS-A_2126	FM AMTS: Speicherstruktur EF.VerweiseAMTS auf der eGK	gemSpec_eGK_Fach_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2127	FM AMTS: Speicherstruktur EF.StatusAMTS auf der eGK	gemSpec_eGK_Fach_AMTS
AMTS-A_2620	FM AMTS: WriteConsent – Transformationsprozess der Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2621	FM AMTS: ReadConsent – Transformationsprozess der Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2660	FM AMTS: Speicherstruktur EF.EinwilligungAMTS auf der eGK	gemSpec_eGK_Fach_AMTS
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_7330	Tracedaten von echten Außenschnittstellen	gemKPT_Test
TIP1-A_7331	Bereitstellung von Tracedaten an Außenschnittstelle	gemKPT_Test
A_22894	Handbuch Erläuterungen zur Zertifikatsauswahl	gemSpec_Kon
TIP1-A_4710	Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

Tabelle 6: Festlegungen zur funktionalen Eignung "Herstellererklärung" zur Herausgabe der gSMC-K

ID	Bezeichnung	Quelle (Referenz)
A_20065	Nutzung der Dokumententemplates der gematik	gemKPT_Test
GS-A_5020	Einbringung des Komponentenzertifikats durch den Kartenherausgeber	gemRL_TSL_SP_CP
TIP1-A_2575	Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat	gemSpec_CVC_TSP
TIP1-A_2578	Korrekte ICCSN der Chipkarte	gemSpec_CVC_TSP

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_2589	Personalisierung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
Card-G2-A_3479	Kodierung von Versionskennungen	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3480	Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3481	Ausschluss für die Kodierung von Produktidentifikatoren	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3487	K_Initialisierung und K_Personalisierung: DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3492	K_Personalisierung: DO_PT_Pers in EF.ATR	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3494	K_Personalisierung: DO_PI_Kartenkörper in EF.ATR- Personalisierung	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3495	K_Personalisierung: DO_PI_Personalisierung in EF.ATR-Personalisierung	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3496	K_Initialisierung: Weitere Datenobjekte in DO_HistoricalBytes in EF.ATR	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3497	K_Personalisierung: Vollständige Befüllung von EF.ATR	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3498	K_Personalisierung: DO_ICCSN in EF.GDO	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3507	K_Personalisierung Versionierung Inhalte von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP_G2 .1
Card-G2-A_3509	K_Personalisierung Inhalt von EF.EnvironmentSettings	gemSpec_Karten_Fach_TIP_G2 .1
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM

ID	Bezeichnung	Quelle (Referenz)
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS-A_4559	Versionierung der Karten der TI	gemSpec_OM
GS-A_4560	Versionierung von Datenstrukturen der Karten der TI	gemSpec_OM
GS-A_5026	Versionierung von Karten durch die Produktidentifikation	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039-01	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_5140	Inhalt der Selbstauskunft von Karten	gemSpec_OM
GS-A_4605	Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung	gemSpec_PKI
GS-A_4606	Identischer ICCSN in allen Zertifikaten einer gSMC-K	gemSpec_PKI
GS-A_4622-01	Zugriffsprofil einer gSMC-K	gemSpec_PKI
GS-A_4707	Kennzeichen für Technische Rolle für Komponenten und Dienste	gemSpec_PKI
GS-A_4974	CV-Ausstattung von Smartcards der TI	gemSpec_PKI
GS-A_5335-01	Zugriffsprofil einer gSMC-K für Administrationszwecke	gemSpec_PKI
Card-G2-A_2538	K_Initialisierung: Anzahl logischer Kanäle	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_2541	K_Personalisierung: zusätzliche Ordner	gemSpec_gSMC-K_ObjSys
Card-G2-A_2542	K_Personalisierung: zusätzliche Objekte	gemSpec_gSMC-K_ObjSys
Card-G2-A_2544	K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset	gemSpec_gSMC-K_ObjSys
Card-G2-A_2545	K_Personalisierung: Wert des Attributes iccsn8	gemSpec_gSMC-K_ObjSys
Card-G2-A_2547	K_Personalisierung und K_Initialisierung: ATR-Kodierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_2548	K_Personalisierung und K_Initialisierung: TC1 Byte im ATR	gemSpec_gSMC-K_ObjSys
Card-G2-A_2567	K_Personalisierung: Personalisiertes Attribut von EF.GDO	gemSpec_gSMC-K_ObjSys
Card-G2-A_2570	K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_2638	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_2640	K_Personalisierung: CHR von C.SAK.AUTD_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_2665	K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“	gemSpec_gSMC-K_ObjSys
Card-G2-A_2994	K_Personalisierung: Absicherung der Kartenadministration	gemSpec_gSMC-K_ObjSys
Card-G2-A_2997	K_Personalisierung und K_Initialisierung: Historical Bytes im ATR	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3041	K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes	gemSpec_gSMC-K_ObjSys
Card-G2-A_3201	K_Personalisierung und K_Initialisierung: Zuordnung zu transportStatus für die Passwortobjekte der gSMC-K	gemSpec_gSMC-K_ObjSys
Card-G2-A_3261	K_Initialisierung und K_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung	gemSpec_gSMC-K_ObjSys
Card-G2-A_3262-01	K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3328	K_Personalisierung: Festlegung von CHR für EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3329	K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3331	K_externe Welt: Festlegung von CHR für EF.C.SMC.AUT_CVC.E384	gemSpec_gSMC-K_ObjSys
Card-G2-A_3333	K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUT_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3336	K_Initialisierung und K_Personalisierung: Vorgaben für die Option_Erweiterung_herstellerspezifische_Schlüssel_01	gemSpec_gSMC-K_ObjSys
Card-G2-A_3338	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3376	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3380	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3382	K_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048 (Option_Erweiterung_herstellerspezifische_Schlüssel_01)	gemSpec_gSMC-K_ObjSys
Card-G2-A_3394	K_Personalisierung: Personalisierte Attribute von MF / EF.EnvironmentSettings	gemSpec_gSMC-K_ObjSys
Card-G2-A_3396	K_Personalisierung: Personalisierte Attribute von MF / PIN.AK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3397	K_Personalisierung: Personalisierte Attribute von MF / PIN.NK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3398	K_Personalisierung: Personalisierte Attribute von MF / PIN.Pers	gemSpec_gSMC-K_ObjSys
Card-G2-A_3399	K_Personalisierung: Personalisierte Attribute von MF / PIN.SAK	gemSpec_gSMC-K_ObjSys
Card-G2-A_3400	K_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3401	K_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3402	K_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3404	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES128	gemSpec_gSMC-K_ObjSys
Card-G2-A_3405	K_Personalisierung: Personalisierte Attribute von MF / SK.CMS.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3406	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3407	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA_PS.R2048	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3410	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3411	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3416	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3417	K_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3423	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3424	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3429	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3430	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD_CVC.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3431	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA_xTV.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3434	K_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3438	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetZA_RCA	gemSpec_gSMC-K_ObjSys
Card-G2-A_3439	K_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL_CA	gemSpec_gSMC-K_ObjSys
Card-G2-A_3447	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES128	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3449	K_Personalisierung: Personalisierte Attribute von MF / SK.CUP.AES256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3450	K_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048	gemSpec_gSMC-K_ObjSys
Card-G2-A_3514	K_Personalisierung: personalisierter Wert von pointInTime	gemSpec_gSMC-K_ObjSys
Card-G2-A_3580	K_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3581	K_Personalisierung: Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3583-01	K_Personalisierung: Personalisierte Attribute von MF / EF.C.TSL.CA_1 für Testkarten	gemSpec_gSMC-K_ObjSys
Card-G2-A_3734	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/EF.C.AK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3735	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/PrK.AK.AUT.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3738	K_Personalisierung: Personalisierte Attribute von MF/DF.AK/PrK.AK.CA_PS.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3740	K_Personalisierung: Personalisierte Attribute von MF/DF.NK/EF.C.NK.VPN2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3741	K_Personalisierung: Personalisierte Attribute von MF/DF.NK/PrK.NK.VPN.E256	gemSpec_gSMC-K_ObjSys
Card-G2-A_3744	K_Personalisierung: Personalisierte Attribute von MF/DF.SAK/EF.C.SAK.AUT2.XXXX	gemSpec_gSMC-K_ObjSys
Card-G2-A_3745	K_Personalisierung: Personalisierte Attribute von MF/DF.SAK/PrK.SAK.AUT.E256	gemSpec_gSMC-K_ObjSys

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3850	K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung	gemSpec_gSMC-K_ObjSys
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

3.2 Festlegungen zur sicherheitstechnischen Eignung

Die sicherheitstechnische Eignung des Produktes wird durch das Zusammenspiel von drei Nachweisen erreicht:

- Beschleunigte Sicherheitszertifizierung durch das BSI
- Prüfung durch CC-Prüfstelle mit Abnahme durch die gematik
- Produktgutachten mit Abnahme durch die gematik.

Bei Verwendung eines HSM für die Konnektoridentität kommt als vierter Nachweis ein Sicherheitsgutachten für die Personalisierung hinzu.

Zudem muss der Hersteller seine sicheren Softwareentwicklungsprozesse durch ein Sicherheitsgutachten nachweisen.

3.2.1 Beschleunigte Sicherheitszertifizierung (BSZ)

Es ist eine Beschleunigte Sicherheitszertifizierung durch das BSI gefordert, wobei eine Prüfung durch eine vom BSI für den Geltungsbereich Highspeedkonnektor anerkannte Prüfstelle beauftragt werden muss.

Es handelt sich grundsätzlich um einen Black-Box-Ansatz mit einem starken Fokus auf Penetrationstests. Jedoch findet insbesondere für den Bereich Kryptographie auch in der BSZ eine Prüfung anhand von Quellcode statt.

Zudem wird über die Pentests der Außenschnittstellen hinaus die Prüfung der korrekten Implementierungen von sicherheitsrelevanten Kommunikationsprotokollen innerhalb der BSZ vorgenommen.

Die Festlegungen zum BSZ-Geltungsbereich HSK finden in BSI-Dokumenten statt.

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Beschleunigte Sicherheitszertifizierung (BSZ)"

ID	Bezeichnung	Quelle (Referenz)
A_21988-01	Highspeed-Konnektor - Keine zusätzlichen Schnittstellen	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
A_23474	Nachnutzung HSM durch TI-GW-Zugangsmodul - Absicherung und Prüfung	gemF_Highspeed-Konnektor
TIP1-A_4814-02	Export- Import von Konfigurationsdaten	gemF_Highspeed-Konnektor
VSDM-A_2637	Fachmodul VSDM: Zugriff nur für autorisierte Personen	gemSpec_FM_VSDM
A_14223	FM ePA: Autorisierung - Verbindung mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_14930	FM ePA: Authentisierung mit eGK - TLS mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_15532	FM ePA: Dokumentenverwaltung - TLS mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_17948	FM ePA: Authentisierung mit eGK - TLS-Verbindung - Fehler	gemSpec_FM_ePA
A_18011	FM ePA: Schlüsselableitung - TLS-Verbindung zu SGD 1 und 2 aufbauen	gemSpec_FM_ePA
A_18012	FM ePA: Schlüsselableitung- TLS mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_17661	Gesicherte Übertragung der Hash-Datei für TSL (ECC-Migration)	gemSpec_Kon
A_21697-01	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	gemSpec_Kon
A_21698	Importiertes Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon
A_21699-02	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
A_21701	X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen exportieren	gemSpec_Kon
A_21702	Intern generierte Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_21760-01	ID.AK.AUT auf gSMC-K für Authentisierung des Konnektors gegenüber Clientsystemen verwenden	gemSpec_Kon
TIP1-A_4507	Isolation während der Bootup-Phase	gemSpec_Kon
TIP1-A_4515	Verpflichtung zur Nutzung der TLS-Verbindung	gemSpec_Kon
TIP1-A_4516	Authentifizierung der Clients über Basic-Auth und X.509-Zertifikate	gemSpec_Kon
TIP1-A_4517-02	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4518-02	Konfiguration der Anbindung Clientsysteme	gemSpec_Kon
TIP1-A_4524-03	TUC_KON_000 „Prüfe Zugriffsberechtigung“	gemSpec_Kon
TIP1-A_4545-03	TUC_KON_050 „Beginne Kartenterminalsitzung“	gemSpec_Kon
TIP1-A_4595	Gesicherte Übertragung von Ereignissen	gemSpec_Kon
TIP1-A_4720-02	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	gemSpec_Kon
TIP1-A_4806-01	Verpflichtende Managementschnittstelle	gemSpec_Kon
TIP1-A_4808-01	Zugangsschutz der Managementschnittstelle	gemSpec_Kon
TIP1-A_4818	Konfigurieren von Fachmodulen	gemSpec_Kon
TIP1-A_4834	TUC_KON_282 „UpdateInformationen beziehen“	gemSpec_Kon
TIP1-A_5009	Authentifizierungsvarianten für Verbindungen zwischen Konnektor und Clientsystemen	gemSpec_Kon
TIP1-A_5517-02	Konnektor, TUC_KON_290 „LDAP-Verbindung aufbauen“	gemSpec_Kon
TIP1-A_5661	Automatisierung Managementschnittstelle	gemSpec_Kon
TIP1-A_5662	Gesicherte Übertragung von BNetzA-VL und Hashwert	gemSpec_Kon
TIP1-A_7254	Reaktion auf OCSP-Abfrage beim TLS-Verbindungsaufbau	gemSpec_Kon
A_17094-01	TLS-Verbindungen Konnektor (ECC-Migration)	gemSpec_Krypt
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
GS-A_4384-01	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5345-01	TLS-Verbindungen Konnektor	gemSpec_Krypt
GS-A_5525	TLS-Renegotiation Konnektor	gemSpec_Krypt
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
VSDM-A_3003	Verschlüsselter Transport durch Fachmodul VSDM	gemSpec_SST_VSDM
TIP1-A_5566	LDAP Client, LDAPS	gemSpec_VZD
A_21988	Highspeed-Konnektor—Keine zusätzlichen Schnittstellen	gemF_Highspeed-Konnektor
A_21697	Schlüsselpaar und dazugehöriges X.509-Zertifikat für Authentisierung des Konnektors gegenüber Clientsystemen importieren	gemSpec_Kon
A_21699-01	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4806	Verpflichtende Managementschnittstelle	gemSpec_Kon

3.2.2 Prüfung durch CC-Prüfstelle

Ziel dieses Prüfverfahrens ist es mittels Quellcode-Analyse und funktionalen Tests die Umsetzung der Sicherheitsfunktionen zu prüfen, deren Umsetzung sich weniger gut durch den Pentest-Ansatz der BSZ überprüfen lässt.

Es muss eine vom BSI anerkannte Common-Criteria-Prüfstelle mit Konnektor-Erfahrung beauftragt werden. Konkret muss ein Evaluator mit Konnektor-Erfahrung zum Einsatz kommen.

Der Prüfbericht der Prüfstelle wird bei der gematik eingereicht, von der gematik geprüft und im Positivfall abgenommen.

Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Prüfung durch CC-Prüfstelle"

ID	Bezeichnung	Quelle (Referenz)
A_17548-02	TSL-Signer-CA Zertifikat sicher speichern	gemF_Highspeed-Konnektor
A_21882	Authentisierung für Kopplung von Konnektor und SZSP	gemF_Highspeed-Konnektor
A_21987	Zugriff auf die VAU nur durch den Hersteller	gemF_Highspeed-Konnektor
A_22041	Highspeed-Konnektor: Sichere Trennung virtueller Instanzen	gemF_Highspeed-Konnektor
A_22338	Tägliche Aktualisierung der TSL	gemF_Highspeed-Konnektor
A_23303	TLS mit Client-Authentisierung verpflichtend für Clientsystemanbindungen	gemF_Highspeed-Konnektor
A_23359	Administration des HSK-Basis Systems	gemF_Highspeed-Konnektor
A_23360	TI-Gateway - Kopplung Zugangsmodul und HSK	gemF_Highspeed-Konnektor
A_23395	Backup & Restore von Instanzen (Konfigurationsdaten)	gemF_Highspeed-Konnektor
A_23397	Sicherung und Wiederherstellung HSK-Basisystem	gemF_Highspeed-Konnektor
A_23432	Verpflichtendes Auto-Update	gemF_Highspeed-Konnektor
TIP1-A_4503-03	Verpflichtung zur Nutzung von gSMC-K oder HSM	gemF_Highspeed-Konnektor
TIP1-A_4693-03	TUC_KON_032 „TSL aktualisieren“	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4730-02	Kommunikation mit NET_TI_GESICHERTE_FD	gemF_Highspeed-Konnektor
TIP1-A_4731-02	Kommunikation mit NET_TI_ZENTRAL	gemF_Highspeed-Konnektor
TIP1-A_4732-02	Kommunikation mit NET_TI_DEZENTRAL	gemF_Highspeed-Konnektor
TIP1-A_4810-02	Benutzerverwaltung der Managementschnittstelle	gemF_Highspeed-Konnektor
TIP1-A_4820-02	HSK: Instanzen erstellen und löschen	gemF_Highspeed-Konnektor
TIP1-A_4832-03	TUC_KON_280 „Konnektoraktualisierung durchführen“	gemF_Highspeed-Konnektor
A_14975-01	Verschlüsselung des Dokuments mit dem DocumentKey	gemSpec_DM_ePA
A_14976-02	Verschlüsselung des DocumentKey mit dem RecordKey	gemSpec_DM_ePA
A_15592-03	Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls	gemSpec_Dokumentenverwaltung
AMTS-A_2139	FM AMTS: Verbot Protokollierung Schlüsselmaterial	gemSpec_FM_AMTS
AMTS-A_2140	FM AMTS: Verbot Protokollierung personenbezogener Daten	gemSpec_FM_AMTS
AMTS-A_2167	FM AMTS: Übergreifende Anforderung – Keine Nutzung der Privat-PIN	gemSpec_FM_AMTS
AMTS-A_2169	FM AMTS: Übergreifende Anforderung – Versicherten-ID im Cache löschen	gemSpec_FM_AMTS
AMTS-A_2189	FM AMTS: Übergreifende Anforderung – Kein Caching der eMP/AMTS-Daten	gemSpec_FM_AMTS
AMTS-A_2192	FM AMTS: ReadMP – PIN zur Freischaltung von EF.AMTS	gemSpec_FM_AMTS
AMTS-A_2202	FM AMTS: WriteMP – PIN zur Freischaltung von EF.AMTS	gemSpec_FM_AMTS
AMTS-A_2648	FM AMTS: Übergreifende Anforderung – Löschung von zwischengespeicherten eMP/AMTS-Daten	gemSpec_FM_AMTS
NFDM-A_2095	Verbot Protokollierung medizinischer Daten	gemSpec_FM_NFDM

ID	Bezeichnung	Quelle (Referenz)
NFDM-A_2096	Verbot Protokollierung Schlüsselmaterial	gemSpec_FM_NFDM
NFDM-A_2097	Verbot Protokollierung personenbezogener Daten	gemSpec_FM_NFDM
NFDM-A_2105	Verbot der persistenten Speicherung medizinischer Daten	gemSpec_FM_NFDM
NFDM-A_2112	Berechtigungsregeln ReadNFD	gemSpec_FM_NFDM
NFDM-A_2115	Berechtigungsregeln WriteNFD	gemSpec_FM_NFDM
NFDM-A_2118	Berechtigungsregeln EraseNFD	gemSpec_FM_NFDM
NFDM-A_2122	Berechtigungsregeln ReadDPE	gemSpec_FM_NFDM
NFDM-A_2125	Berechtigungsregeln WriteDPE	gemSpec_FM_NFDM
NFDM-A_2128	Berechtigungsregeln EraseDPE	gemSpec_FM_NFDM
VSDM-A_2789	Fachmodul VSDM: keine Protokollierung von Schlüsselmaterial	gemSpec_FM_VSDM
A_13677	FM ePA: Aktensession - Trennung von Operation	gemSpec_FM_ePA
A_13903	FM ePA: putDocuments - Löschen der Dokumentenschlüssel	gemSpec_FM_ePA
A_13907	FM ePA: putDocuments - Verschlüsselung der Dokumente	gemSpec_FM_ePA
A_13941	FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen	gemSpec_FM_ePA
A_14154	FM ePA: Verbot des Logging von Schlüsselmaterial	gemSpec_FM_ePA
A_14155	FM ePA: Verbot des Logging von medizinischen und personenbezogenen Daten	gemSpec_FM_ePA
A_14173	FM ePA: Sicherheit - Keine persistente Speicherung von personenbezogenen Daten	gemSpec_FM_ePA
A_14174	FM ePA: Sicherheit - Keine Speicherung von privaten Schlüsseln	gemSpec_FM_ePA
A_14175	FM ePA: Sicherheit - Keine Weitergabe vertraulicher Informationsobjekte an das PS	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_14651	FM ePA: Logout Aktensession - Löschung der Aktensession	gemSpec_FM_ePA
A_14710	FM ePA: Übergreifende Anforderung - Verwendung des Protokollierungsdienstes	gemSpec_FM_ePA
A_14722	FM ePA: Sicherheit - Keine persistente Speicherung von Dokumenten und Metadaten	gemSpec_FM_ePA
A_14742	FM ePA: ActivateAccount - Akten- und Kontextschlüssel erzeugen	gemSpec_FM_ePA
A_14748	FM ePA: Übergreifende Anforderung - Verwendung des Verschlüsselungsdienstes	gemSpec_FM_ePA
A_14769	FM ePA: RequestFacilityAuthorization - Bestätigung der Berechtigung	gemSpec_FM_ePA
A_14927	FM ePA: Authentisierung mit SM-B - Erstellung des SAML-Token	gemSpec_FM_ePA
A_14959	FM ePA: getDocuments - Löschen der Dokumentenschlüssel	gemSpec_FM_ePA
A_15135	FM ePA: Übergreifende Anforderung - Verwendung des Namensdienstes	gemSpec_FM_ePA
A_15136	FM ePA: Übergreifende Anforderung - Verwendung des Zugriffsberechtigungsdienstes	gemSpec_FM_ePA
A_15194	FM ePA: Übergreifende Anforderung - Verwendung des Kartendienstes	gemSpec_FM_ePA
A_15199-01	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Verfahren	gemSpec_FM_ePA
A_15210	FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU mit Zertifikats- und Rollenprüfung	gemSpec_FM_ePA
A_15215	FM ePA: Übergreifende Anforderung - Prüfung von Authentizität und Echtheit der beteiligten Smartcards (C2C)	gemSpec_FM_ePA
A_15535	FM ePA: Übergreifende Anforderung - Verwendung des TLS-Dienstes des Konnektors	gemSpec_FM_ePA
A_15638	FM ePA: Authentisierung mit SM-B - Behauptungen im SAML-Token	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_15677	FM ePA: Übergreifende Anforderung - Verwendung des Zeitdienstes des Konnektors	gemSpec_FM_ePA
A_15693	FM ePA: RequestFacilityAuthorization - Erstellung von Policy Document	gemSpec_FM_ePA
A_15693-05	FM ePA: RequestFacilityAuthorization Version 2.x - Erstellung von Policy Document	gemSpec_FM_ePA
A_15867	FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Schlüsselerzeugung	gemSpec_FM_ePA
A_15891	FM ePA: Übergreifende Anforderung - Verwendung des Zertifikatsdienstes	gemSpec_FM_ePA
A_15892	FM ePA: Übergreifende Anforderung - Verwendung des Signaturdienstes	gemSpec_FM_ePA
A_15894	FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit der VAU bei Schlüsselaushandlung	gemSpec_FM_ePA
A_15895	FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit der VAU bei Schlüsselableitung	gemSpec_FM_ePA
A_16193	FM ePA: Übergreifende Anforderung - Vorgaben Aktenschlüssel und Kontextschlüssel - Fehler	gemSpec_FM_ePA
A_17868	FM ePA: RequestFacilityAuthorization - Akten- und Kontextschlüssel mit eGK verschlüsseln	gemSpec_FM_ePA
A_17879	FM ePA: Übergreifende Anforderung IHE - Außenverhalten der IHE ITI-Implementierung	gemSpec_FM_ePA
A_17949-01	FM ePA: Aktensession - Löschen der Aktensession bei Entfernen der eGK	gemSpec_FM_ePA
A_17966	FM ePA: Schlüsselableitung - Ablauf	gemSpec_FM_ePA
A_17988	FM ePA: RequestFacilityAuthorization - Schlüsselableitung in Abhängigkeit von der Rolle	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_18007	Schlüsselableitung bei Verschlüsselung - Verschlüsselung mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18008	FM ePA: putDocuments - Verschlüsselung der Dokumente mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18165	FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit einem SGD	gemSpec_FM_ePA
A_20157	Übergreifende Anforderung – Unterbindung paralleler Zugriff auf die eGK (Reservierung)	gemSpec_FM_ePA
A_17225-01	Aufbau einer sicheren Verbindung zur Vertrauenswürdige Ausführungsumgebung (VAU)	gemSpec_Kon
A_17746	Einsatzbereich und Vorgaben für Ver- und Entschlüsselung (ECC-Migration)	gemSpec_Kon
A_17768	Zertifikate und Schlüssel für Signaturerstellung und Signaturprüfung (QES und nonQES)	gemSpec_Kon
A_17777	sicherheitstechnische Festlegungen zum Abruf von kryptographischen Schlüsseln von einem Schlüsselgenerierungsdienst	gemSpec_Kon
A_18001	TUC_KON_075 „Symmetrisch verschlüsseln“	gemSpec_Kon
A_18686-01	Komfortsignatur-Timer	gemSpec_Kon
A_18756	Optionalität von nonQES-XAdES Signatur	gemSpec_Kon
A_19052-01	Mindestanforderungen an Dokumente und Nachrichten	gemSpec_Kon
A_19100-01	Komfortsignatur-Zähler	gemSpec_Kon
A_19101	Handbuch-Hinweis zu Nutzerauthentisierung am Clientsystem bei Komfortsignatur	gemSpec_Kon
A_19102-04	TUC_KON_158 „Komfortsignaturen erstellen“	gemSpec_Kon
A_19103-07	TUC_KON_170 "Dokumente mit Komfort signieren"	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
A_19104-04	TUC_KON_171 „Komfortsignatur einschalten“	gemSpec_Kon
A_19105	TUC_KON_172 „Komfortsignatur ausschalten“	gemSpec_Kon
A_19106-02	TUC_KON_173 „Liefere Signaturmodus“	gemSpec_Kon
A_19109-02	Operation GetSignatureMode	gemSpec_Kon
A_19258	Secure Messaging bei Komfortsignatur	gemSpec_Kon
A_20073-01	Prüfung der Länge der UserId	gemSpec_Kon
A_20074	UserId über 1.000 Vorgänge eindeutig	gemSpec_Kon
A_21699-02	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
A_22344	Mindestens zwei parallele Komfortsignatursessions für einen HBA	gemSpec_Kon
A_22352	Unabhängige Komfortsignatur-Timer bei parallelen Komfortsignatursessions	gemSpec_Kon
A_22459	Unabhängige Komfortsignatur-Zähler bei parallelen Komfortsignatursessions	gemSpec_Kon
A_22673	Unerlaubte Inhalte in Dokumenten und Nachrichten	gemSpec_Kon
A_22923	XML-Attribute schemaLocation und noNamespaceSchemaLocation nicht auswerten	gemSpec_Kon
A_23311	HBA Prüfung bei Steckvorgang	gemSpec_Kon
A_23536	TUC_KON_159 - "Signaturdatenelemente nachbereiten"	gemSpec_Kon
A_23614	SMC-B Prüfung bei Steckvorgang	gemSpec_Kon
A_23702	Keine Verzögerungen durch Prüfungen bei Steckvorgang	gemSpec_Kon
TIP1-A_4509	Betriebszustand erfassen	gemSpec_Kon
TIP1-A_4510-05	Sicherheitskritische Fehlerzustände	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4517-02	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4524-03	TUC_KON_000 „Prüfe Zugriffsberechtigung“	gemSpec_Kon
TIP1-A_4527-04	TUC_KON_080 „Dokument validieren“	gemSpec_Kon
TIP1-A_4545-03	TUC_KON_050 „Beginne Kartenterminalsitzung“	gemSpec_Kon
TIP1-A_4548-02	TUC_KON_053 „Paire Kartenterminal“	gemSpec_Kon
TIP1-A_4558	Caching-Dauer von Kartendaten im Konnektor	gemSpec_Kon
TIP1-A_4559	Konnektorzugriffsverbot auf DF.KT	gemSpec_Kon
TIP1-A_4560	Rahmenbedingungen für Kartensitzungen	gemSpec_Kon
TIP1-A_4565	TUC_KON_001 „Karte öffnen“	gemSpec_Kon
TIP1-A_4566	TUC_KON_026 „Liefere CardSession“	gemSpec_Kon
TIP1-A_4567	TUC_KON_012 „PIN verifizieren“	gemSpec_Kon
TIP1-A_4571	TUC_KON_023 „Karte reservieren“	gemSpec_Kon
TIP1-A_4572	TUC_KON_005 „Card-to-Card authentisieren“	gemSpec_Kon
TIP1-A_4579	TUC_KON_018 „eGK-Sperrung prüfen“	gemSpec_Kon
TIP1-A_4581	TUC_KON_218 „Signiere“	gemSpec_Kon
TIP1-A_4582	TUC_KON_219 „Entschlüssele“	gemSpec_Kon
TIP1-A_4584	TUC_KON_024 „Karte zurücksetzen“	gemSpec_Kon
TIP1-A_4616-03	TUC_KON_070 „Daten hybrid verschlüsseln“	gemSpec_Kon
TIP1-A_4617-02	TUC_KON_071 „Daten hybrid entschlüsseln“	gemSpec_Kon
TIP1-A_4623-02	Unterstützte Signaturverfahren nonQES	gemSpec_Kon
TIP1-A_4627	Unterstützte Signaturverfahren QES	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4639	Generierung von Jobnummern für PIN-Eingaben	gemSpec_Kon
TIP1-A_4640	Anzeige der Jobnummern für PIN-Eingaben	gemSpec_Kon
TIP1-A_4642	Ableitung der Jobnummer von einem Zufallswert	gemSpec_Kon
TIP1-A_4644	Jobnummer über 1.000 Vorgänge eindeutig	gemSpec_Kon
TIP1-A_4647-03	TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“	gemSpec_Kon
TIP1-A_4648	TUC_KON_166 „nonQES Signaturen erstellen“	gemSpec_Kon
TIP1-A_4649-02	TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	gemSpec_Kon
TIP1-A_4651-02	TUC_KON_154 „QES Signaturen erstellen“	gemSpec_Kon
TIP1-A_4652-02	TUC_KON_168 „Einzelsignatur QES erstellen“	gemSpec_Kon
TIP1-A_4653-03	TUC_KON_160 „Dokumente nonQES signieren“	gemSpec_Kon
TIP1-A_4654-05	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	gemSpec_Kon
TIP1-A_4655-03	TUC_KON_150 „Dokument QES signieren“	gemSpec_Kon
TIP1-A_4670	Secure Messaging für die DTBS	gemSpec_Kon
TIP1-A_4671	Verhalten des Konnektors beim Abbruch einer Stapelsignatur	gemSpec_Kon
TIP1-A_4672-05	TUC_KON_151 „QES-Dokumentensignatur prüfen“	gemSpec_Kon
TIP1-A_4680-03	Konfigurationswerte des Signatordienstes	gemSpec_Kon
TIP1-A_4682	Sicheres Einbringen des TI-Vertrauensankers	gemSpec_Kon
TIP1-A_4696-03	TUC_KON_037 „Zertifikat prüfen“	gemSpec_Kon
TIP1-A_4709	Integrität des Sicherheitsprotokolls	gemSpec_Kon
TIP1-A_4710-02	Keine Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4715	TUC_KON_271 „Schreibe Protokolleintrag“	gemSpec_Kon
TIP1-A_4716	Einsichtnahme und Veränderung der Protokolle	gemSpec_Kon
TIP1-A_4788	Verhalten bei Abweichung zwischen lokaler Zeit und erhaltenen Zeit	gemSpec_Kon
TIP1-A_4812	Anzeige der Versionsinformationen (Selbstauskunft)	gemSpec_Kon
TIP1-A_4813	Persistieren der Konfigurationsdaten	gemSpec_Kon
TIP1-A_4815	Export: Schutz der Integrität, Authentizität und Nichtabstreitbarkeit	gemSpec_Kon
TIP1-A_4816	Export: Schutz der Vertraulichkeit	gemSpec_Kon
TIP1-A_4992-02	Guidance zur Jobnummer	gemSpec_Kon
TIP1-A_5011	Import von Kartenterminal-Informationen	gemSpec_Kon
TIP1-A_5012	Remote-PIN-Verfahren	gemSpec_Kon
TIP1-A_5433	Manuell importierte X.509-CA-Zertifikate nur für hybride Verschlüsselung	gemSpec_Kon
TIP1-A_5437-02	Signaturverfahren für externe Authentisierung	gemSpec_Kon
TIP1-A_5447	Einsatzbereich der Signaturvarianten	gemSpec_Kon
TIP1-A_5482-01	TUC_KON_042 „CV-Zertifikat prüfen“	gemSpec_Kon
TIP1-A_5538	Signaturreichtlinien bei QES für XML-Dokumentenformate	gemSpec_Kon
TIP1-A_5540-01	QES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt	gemSpec_Kon
TIP1-A_5541-01	Referenzen in Dokumenten nicht dynamisch auflösen	gemSpec_Kon
TIP1-A_5545	nonQES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt	gemSpec_Kon
TIP1-A_5654	Sicherheits-Protokollierung	gemSpec_Kon
TIP1-A_6478	Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein	gemSpec_Kon
TIP1-A_6729	TUC_KON_031 „BNetzA-VL aktualisieren“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	gemSpec_Kon
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	gemSpec_Kon
TIP1-A_7279	Authentifizierung des Remote-Administrators	gemSpec_Kon
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	gemSpec_Kon
A_15549	VAU-Client: Kommunikation zwischen VAU-Client und VAU	gemSpec_Krypt
A_15705	Vorgaben Aktenschlüssel (RecordKey) und Kontextschlüssel (ContextKey)	gemSpec_Krypt
A_16849	VAU-Protokoll: Aktionen bei Protokollabbruch	gemSpec_Krypt
A_16852-01	VAU-Protokoll: ECDH durchführen	gemSpec_Krypt
A_16883-01	VAU-Protokoll: Aufbau VAUClientHello-Nachricht	gemSpec_Krypt
A_16884	VAU-Protokoll: Nachrichtentypen und HTTP-Content-Type	gemSpec_Krypt
A_16900	VAU-Protokoll: Client, Behandlung von Fehlernachrichten	gemSpec_Krypt
A_16903	VAU-Protokoll: Client, Prüfung des VAUClientHelloDataHash-Werts (aus VAUServerHelloData)	gemSpec_Krypt
A_16941-01	VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData	gemSpec_Krypt
A_16943-01	VAU-Protokoll: Schlüsselableitung (HKDF)	gemSpec_Krypt
A_16945-02	VAU-Protokoll: Client, verschlüsselte Kommunikation (1)	gemSpec_Krypt
A_16957-01	VAU-Protokoll: Client, verschlüsselte Kommunikation (2)	gemSpec_Krypt
A_17069	VAU-Protokoll: Client Zählerüberlauf	gemSpec_Krypt
A_17070-02	VAU-Protokoll: Aufbau der VAUClientSigFin-Nachricht	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_17071	VAU-Protokoll: Versand der VAUClientSigFin-Nachricht	gemSpec_Krypt
A_17074	VAU-Protokoll: Ignorieren von zusätzlichen Datenfeldern in Protokoll-Nachrichten	gemSpec_Krypt
A_17081	VAUProtokoll: zu verwendende Signaturschlüssel	gemSpec_Krypt
A_17084	VAU-Protokoll: Empfang der VAUServerFin-Nachricht	gemSpec_Krypt
A_17094-01	TLS-Verbindungen Konnektor (ECC-Migration)	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt
A_17208	Signaturen von PDF/A-Dokumenten (ECC-Migration)	gemSpec_Krypt
A_17209	Signaturverfahren für externe Authentisierung (ECC-Migration)	gemSpec_Krypt
A_17220	Verschlüsselung binärer Daten (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17221-01	XML-Verschlüsselung (ECIES) (ECC-Migration)	gemSpec_Krypt
A_17359	Signaturen binärer Daten (Dokumente) (ECC-Migration)	gemSpec_Krypt
A_17360	XML-Signaturen (Dokumente) (ECC-Migration)	gemSpec_Krypt
A_17872	Ver- und Entschlüsselung der Akten und Kontextschlüssel (Schlüsselableitungsfunktionalität ePA)	gemSpec_Krypt
A_17874	SGD-Client, Client-authentisiertes ECIES-Schlüsselpaar	gemSpec_Krypt
A_17875	ECIES-verschlüsselter Nachrichtenversand zwischen SGD-Client und SGD-HSM	gemSpec_Krypt
A_18004	Vorgaben für die Kodierung von Chiffraten (innerhalb von ePA)	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_19971	SGD und SGD-Client, Hashfunktion für Signaturerstellung und -prüfung	gemSpec_Krypt
A_23273	VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData, Gültigkeit von OCSP-Antworten	gemSpec_Krypt
A_23282	VAU-Protokoll: Signaturen im VAU-Protokoll	gemSpec_Krypt
GS-A_4357-02	X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen	gemSpec_Krypt
GS-A_4358-01	X.509-Identitäten für die Erstellung und Prüfung qualifizierter elektronischer Signaturen	gemSpec_Krypt
GS-A_4359-02	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4361-02	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	gemSpec_Krypt
GS-A_4362-02	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4365-02	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366-02	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4371-02	XML-Signaturen für nicht-qualifizierte Signaturen	gemSpec_Krypt
GS-A_4372-02	XML-Signaturen für qualifizierte elektronische Signaturen	gemSpec_Krypt
GS-A_4373	XML-Verschlüsselung - symmetrisch	gemSpec_Krypt
GS-A_4374	XML-Verschlüsselung - Hybrid	gemSpec_Krypt
GS-A_4376-02	XML-Verschlüsselung - Hybrid, Schlüsseltransport RSAES-OAEP	gemSpec_Krypt
GS-A_4379	Card-to-Card-Authentisierung G2	gemSpec_Krypt
GS-A_4384-01	TLS-Verbindungen	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
GS-A_4389	Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt
GS-A_4390	Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt
GS-A_4393	Algorithmus bei der Erstellung von Hashwerten von Zertifikaten oder öffentlichen Schlüsseln	gemSpec_Krypt
GS-A_5016	Symmetrische Verschlüsselung binärer Daten	gemSpec_Krypt
GS-A_5071-01	kryptographische Vorgaben für eine Signaturprüfung in der SAK-Konnektor	gemSpec_Krypt
GS-A_5080-01	Signaturen binärer Daten (Dokumente)	gemSpec_Krypt
GS-A_5081-01	Signaturen von PDF/A-Dokumenten	gemSpec_Krypt
GS-A_5207	Signaturverfahren beim initialen Pairing zwischen Konnektor und eHealth-Kartenterminal	gemSpec_Krypt
GS-A_5345-01	TLS-Verbindungen Konnektor	gemSpec_Krypt
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4648	TUC_PKI_019: Prüfung der Aktualität der TSL	gemSpec_PKI
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	gemSpec_PKI
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	gemSpec_PKI
GS-A_4829	TUCs, Fehlerbehandlung	gemSpec_PKI
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4943	Alter der OCSP-Responses für eGK-Zertifikate	gemSpec_PKI
GS-A_5484	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
A_17847	Prüfung eines SGD-HSM-Zertifikats (1/2)	gemSpec_SGD_ePA
A_17848	Prüfung eines SGD-HSM-Zertifikats (2/2)	gemSpec_SGD_ePA
A_17888	SGD, KeyDerivation (Client)	gemSpec_SGD_ePA
A_17892	Aufwärtskompatibilität JSON-Requests und -Responses	gemSpec_SGD_ePA
A_17897	SGD-Client, Anfrage GetPublicKey (Client)	gemSpec_SGD_ePA
A_17899	SGD-Clients, Auswertung der Kodierung des öffentlichen ECIES-Schlüssels eines SGD-HSMs	gemSpec_SGD_ePA
A_17900	SGD-Clients, Kodierung des eigenen kurzlebigen ECIES-Schlüssels	gemSpec_SGD_ePA
A_17901	SGD-Clients, Kodierung der Signatur des eigenen ECIES-Schlüssels	gemSpec_SGD_ePA
A_17902	Kontext SGD, Chiffre-Kodierung beim Nachrichtentransport	gemSpec_SGD_ePA
A_17903	Kontext SGD, Prüfung der ephemeren ECC-Schlüssel des Senders beim ECIES-Verfahren	gemSpec_SGD_ePA
A_17924-01	Anfragen an das SGD-HSM (Client)	gemSpec_SGD_ePA
A_18003	SGD-Client, Prüfung der Telematik-ID bei Berechtigungsvergabe	gemSpec_SGD_ePA
A_18005	SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars	gemSpec_SGD_ePA
A_18006	SGD-Client, KVN	gemSpec_SGD_ePA
A_18024	SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel	gemSpec_SGD_ePA
A_18025-01	SGD-Client, Anfrage GetAuthenticationToken	gemSpec_SGD_ePA
A_18028	SGD-Client, Auswertung der Anfrage GetAuthenticationToken	gemSpec_SGD_ePA
A_18029	SGD-Client, Anfrage KeyDerivation	gemSpec_SGD_ePA
A_18031-01	SGD-Client, Auswertung der Anfrage KeyDerivation (1/2)	gemSpec_SGD_ePA

ID	Bezeichnung	Quelle (Referenz)
A_18032	SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar	gemSpec_SGD_ePA
A_20977	SGD-Client, Auswertung der Anfrage KeyDerivation (2/2)	gemSpec_SGD_ePA
A_22494	SGD-Client, HTTP-Variable SGD-Userpseudonym	gemSpec_SGD_ePA
A_22497	SGD-Client, Mehrfachableitung (kurzlebiges ECIES-Client-Schlüsselpaar)	gemSpec_SGD_ePA
A_22039	Highspeed-Konnektor: Lokaler Kartenleser für gSMC-K und SMC-B möglich	gemF_Highspeed-Konnektor
TIP1-A_4503-02	Verpflichtung zur Nutzung von gSMC-K oder HSM	gemF_Highspeed-Konnektor
A_19103-06	TUC_KON_170 "Dokumente mit Komfort signieren"	gemSpec_Kon
A_21699-01	Schlüssel und X.509-Zertifikate für Authentisierung des Konnektors gegenüber Clientsystemen erzeugen	gemSpec_Kon
TIP1-A_4510-04	Sicherheitskritische Fehlerzustände	gemSpec_Kon
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	gemSpec_Kon
TIP1-A_4647-02	TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“	gemSpec_Kon
TIP1-A_4649	TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	gemSpec_Kon
TIP1-A_4653-02	ab PTV4: TUC_KON_160 „Dokumente nonQES signieren“	gemSpec_Kon
TIP1-A_4654-04	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	gemSpec_Kon
TIP1-A_4655-02	TUC_KON_150 „Dokument QES signieren“	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4672-04	TUC_KON_151 „QES-Dokumentensignatur prüfen“	gemSpec_Kon
TIP1-A_4696-02	TUC_KON_037 „Zertifikat prüfen“	gemSpec_Kon
TIP1-A_4710	Protokollierung personenbezogener und medizinischer Daten	gemSpec_Kon

3.2.3 Produktgutachten

Prüfung von Anforderungen zum Betreiberausschluss und zur VAU entsprechend [gemRL_PruefSichEig_DS]. Das Produktgutachten ist der gematik vorzulegen, wird geprüft und im Positivfall abgenommen.

Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"

ID	Bezeichnung	Quelle (Referenz)
A_17346-01	HSK: Verarbeitungskontext der VAU	gemF_Highspeed-Konnektor
A_17347-01	HSK: Verarbeitungskontext der VAU - Keine persistente Speicherung von Versichertendaten	gemF_Highspeed-Konnektor
A_17348-01	HSK: Verarbeitungskontext der VAU - Akten- und Kontextschlüssel verlassen VAU nie	gemF_Highspeed-Konnektor
A_17350-01	HSK: Isolation der VAU von Datenverarbeitungsprozessen des Anbieters	gemF_Highspeed-Konnektor
A_17351-01	HSK: Ausschluss von Manipulationen an der Software der VAU	gemF_Highspeed-Konnektor
A_17352-01	HSK: Ausschluss von Manipulationen an der Hardware der VAU	gemF_Highspeed-Konnektor
A_17353-01	HSK: Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU	gemF_Highspeed-Konnektor
A_17354-01	HSK: Kein physischer Zugang des Anbieters zu Systemen der VAU	gemF_Highspeed-Konnektor
A_17355-01	HSK: Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU	gemF_Highspeed-Konnektor
A_17356-02	HSK: Löschen aller Daten beim Beenden des Verarbeitungskontextes	gemF_Highspeed-Konnektor

ID	Bezeichnung	Quelle (Referenz)
A_17598-01	Qualität des HSM	gemF_Highspeed-Konnektor
A_21853-01	Feste Kopplung von Konnektor und SZSP	gemF_Highspeed-Konnektor
A_21883	Kopplung von Konnektor und SZSP nur durch Hersteller	gemF_Highspeed-Konnektor
A_21886	Feste Kopplung von Konnektor und HSM	gemF_Highspeed-Konnektor
A_21987	Zugriff auf die VAU nur durch den Hersteller	gemF_Highspeed-Konnektor
A_23474	Nachnutzung HSM durch TI-GW-Zugangsmodule - Absicherung und Prüfung	gemF_Highspeed-Konnektor
A_23495	HSK: Protokollierung bei physischem Zugang zu Systemen der VAU	gemF_Highspeed-Konnektor
A_17356-01	HSK: Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes	gemF_Highspeed-Konnektor
A_22040	Highspeed-Konnektor: Absicherung Anbindung lokaler Kartenleser	gemF_Highspeed-Konnektor

3.2.4 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig_DS]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Die Festlegungen in diesem Kapitel betreffen Personalisierungsprozesse und Softwareentwicklungsprozesse.

Personalisierungsprozesse

Im Folgenden wird zunächst die Herausgabe der gSMC-K oder eines HSM mit der Funktionalität der gSMC-K behandelt. Das Sicherheitsgutachten muss entsprechend die Schlüsselerzeugung, den Zertifikatsbezug und die Personalisierung der Daten auf die gSMC-K oder dem HSM umfassen.

Verwendung einer gSMC-K

Das Vorgehen entspricht jenem beim Inboxkonnektor.

Werden alle Aufgaben vom Personalisierer der gSMC-K erfüllt, ist vom Hersteller ein Sicherheitsgutachten (Tabelle 11) des Personalisierers erforderlich.

Wenn der Hersteller des Konnektors die Schlüssel für die gSMC-K jedoch selber erzeugt oder von einem Dritten (der nicht der Personalisierer ist) erzeugen lässt, ist neben dem Sicherheitsgutachten vom Personalisierer auch vom Hersteller oder dem von ihm

beauftragten Dritten ein entsprechendes Sicherheitsgutachten, das die Schlüsselerzeugung umfasst, einzureichen (basierend auf Tabelle 11 begrenzt auf die sichere Schlüsselerzeugung).

Erzeugt der Hersteller oder ein von ihm beauftragter Dritter ausschließlich „Herstellerspezifische Schlüssel“ sowie Schlüssel zur Kartenadministration (konkret Schlüssel für Objekte der Abschnitte 5.3.20, 5.3.22 und 5.3.23 der Objektsystemspezifikation der gSMC-K G2.0 [gemSpec_gSMC-K_ObjSys]), ist neben dem Sicherheitsgutachten vom Personalisierer eine Herstellererklärung über die Umsetzung der Festlegungen in Tabelle 10 zur Zulassung ausreichend.

Verwendung eines HSM

Der Hersteller muss die sichere Schlüsselerzeugung und Personalisierung des HSM durch ein Sicherheitsgutachten (Tabelle 12) nachweisen.

Tabelle 10: Festlegungen zur Herstellererklärung für die Erzeugung herstellerspezifischer Schlüssel und Admin-Schlüssel durch den Hersteller des Konnektors selbst

ID	Bezeichnung	Quelle (Referenz)
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
TIP1-A_7225	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Kon
TIP1-A_5703	Geschützte Übertragung von Daten zum Kartenpersonalisierer	gemSpec_Kon

Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Personalisierung der gSMC-K

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_2579	Korrektter privater Schlüssel in der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2580	Erzeugung des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_2582	Vertraulichkeit des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	gemSpec_CVC_TSP
TIP1-A_2590	Vernichtung fehlerhafter Chipkarten vor deren Ausgabe	gemSpec_CVC_TSP
TIP1-A_2591	Ausgabe fehlerfreier Chipkarten	gemSpec_CVC_TSP
TIP1-A_4222	Authentizität des öffentlichen Root-Schlüssels	gemSpec_CVC_TSP
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerepezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter

ID	Bezeichnung	Quelle (Referenz)
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_4384-01	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5386	kartenindividuelle geheime und private Schlüssel G2-Karten	gemSpec_Krypt
GS-A_2227	Keine Kartendubletten	gemSpec_PINPUK_TI
GS-A_2228	Trennung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2229	Prozesse und Maßnahmen zur Aushändigung von Karte und PIN/PUK-Brief	gemSpec_PINPUK_TI
GS-A_2230	PIN/PUK-Erzeugung: Länge PIN/PUK (Kartenherausgeber)	gemSpec_PINPUK_TI
GS-A_2232	PIN/PUK-Erzeugung: Verfahren für PIN/PUK-Auswahl	gemSpec_PINPUK_TI
GS-A_2234	PIN/PUK-Erzeugung: Zufallsgenerator für PIN/PUK	gemSpec_PINPUK_TI
GS-A_2235	PIN/PUK-Erzeugung: Ableitung von PIN	gemSpec_PINPUK_TI
GS-A_2236	PIN/PUK-Erzeugung: Ableitung der PIN aus eindeutig dem Versicherten zugeordneten Daten	gemSpec_PINPUK_TI
GS-A_2237	PIN/PUK-Erzeugung: kein Rückschluss von PIN/PUK auf Schlüssel	gemSpec_PINPUK_TI
GS-A_2238	PIN/PUK-Erzeugung: Informationen an Karteninhaber bei selbstständiger Wahl der PIN	gemSpec_PINPUK_TI
GS-A_2239	PIN/PUK-Erzeugung: Ableitung von PIN im Sicherheitsmodul	gemSpec_PINPUK_TI
GS-A_2240	PIN/PUK-Speicherung: Verschlüsselung der PIN außerhalb von Sicherheitsmodulen	gemSpec_PINPUK_TI
GS-A_2242	PIN/PUK-Speicherung: Integrität der PIN außerhalb von Sicherheitsmodulen	gemSpec_PINPUK_TI

ID	Bezeichnung	Quelle (Referenz)
GS-A_2244	PIN/PUK-Speicherung: Verschlüsselung unterschiedlicher PINs mit unterschiedlichen Schlüsseln	gemSpec_PINPUK_TI
GS-A_2246	PIN/PUK-Speicherung: Verschlüsselung gleicher PINs führt zu unterschiedlichen verschlüsselten Werten	gemSpec_PINPUK_TI
GS-A_2247	PIN/PUK-Speicherung: Wiederholte Verschlüsselung der PIN führt zu unterschiedlichen Werten	gemSpec_PINPUK_TI
GS-A_2248	PIN/PUK-Speicherung: unterschiedliche Schlüssel für unterschiedliche Zwecke	gemSpec_PINPUK_TI
GS-A_2249	PIN/PUK-Speicherung: Dokumentation der Zwecke	gemSpec_PINPUK_TI
GS-A_2250	PIN/PUK-Speicherung: Entschlüsselung nur durch berechtigten Empfänger	gemSpec_PINPUK_TI
GS-A_2252	PIN/PUK-Löschung: Löschung von PIN/PUK nach Ablauf der Speicherdauer	gemSpec_PINPUK_TI
GS-A_2253	PIN/PUK-Transport: Sicherer PIN-Transport beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2254	PIN/PUK-Transport: Schutz außerhalb geschützter Hardware beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2255	PIN/PUK-Transport: Verteilung beschränken	gemSpec_PINPUK_TI
GS-A_2256	PIN/PUK-Transport: einmalige PIN-Erstellung beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2260	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls	gemSpec_PINPUK_TI
GS-A_2261	PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls - kein Klartext	gemSpec_PINPUK_TI
GS-A_2264	PIN/PUK-Transport: elektronische PIN-Verteilung	gemSpec_PINPUK_TI
GS-A_2266	PIN/PUK-Transport: Verschlüsselung gleicher PINs muss zu unterschiedlichen Werten führen	gemSpec_PINPUK_TI
GS-A_2270	PIN/PUK-Transport: Unterschiedliche verschlüsselte Werte auch bei gleichen PINs	gemSpec_PINPUK_TI

ID	Bezeichnung	Quelle (Referenz)
GS-A_2271	PIN/PUK-Transport: kein Rückschluss auf vorher benutzte Schlüssel	gemSpec_PINPUK_TI
GS-A_2274	PIN/PUK-Transport: Löschung der PIN nach Transport	gemSpec_PINPUK_TI
GS-A_2276	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip bei der Zuordnung einer PIN/PUK zu einer Karte	gemSpec_PINPUK_TI
GS-A_2277	PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip beim Rücksetzen des Fehlbedienungs Zählers	gemSpec_PINPUK_TI
GS-A_2284	PIN/PUK-Änderung: Änderungen durch Kartenpersonalisierer im Vier-Augen-Prinzip	gemSpec_PINPUK_TI
GS-A_2285	PIN/PUK-Änderung: Prozess bei Kompromittierung beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2287	PIN/PUK-Löschung: Nachweis der Löschung nicht mehr gebrauchter PIN beim Kartenherausgeber bzw. Kartenpersonalisierer	gemSpec_PINPUK_TI
GS-A_2291	PIN/PUK-Löschung: Löschen von nicht mehr benötigten Klartext-PIN	gemSpec_PINPUK_TI
GS-A_2292	PIN/PUK-Löschung: Außerbetriebnahme der PIN und Karte	gemSpec_PINPUK_TI
GS-A_2295	Schutz der Schlüssel für PIN/PUK gemäß Hierarchiestufe 4	gemSpec_PINPUK_TI
GS-A_5085	PIN/PUK-Änderung: Prozess bei Kompromittierungsmeldung durch Karteninhaber	gemSpec_PINPUK_TI
GS-A_5209	PIN/PUK-Speicherung: PIN/PUK unverzüglich löschen	gemSpec_PINPUK_TI
GS-A_5387	Beachten von Vorgaben bei der Kartenpersonalisierung	gemSpec_PINPUK_TI
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys

Zusätzlich ist stets vom Personalisierer und, falls dieser nicht die Schlüssel erzeugt, auch vom Hersteller oder dem von ihm beauftragten Dritten die Herstellererklärung zur Erfüllung der Festlegungen in Kapitel 3.2.5, Tabelle 15 zu erbringen.

Tabelle 12: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Personalisierung des HSM

ID	Bezeichnung	Quelle (Referenz)
A_21885	Personalisierung des HSM mit Konnektidentitäten durch Hersteller	gemF_Highspeed-Konnektor
A_22336	Initialisierung mit ECC-Vertrauensraum	gemF_Highspeed-Konnektor
A_22590	HSK: Kein Abruf von Zertifikatsprofilen C.NK.VPN bei Nutzung HSM	gemF_Highspeed-Konnektor
A_23470	Rollentrennung HSM-Personalisierung und Betrieb TI-Gateway	gemF_Highspeed-Konnektor
TIP1-A_2579	Korrektur privater Schlüssel in der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2580	Erzeugung des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2582	Vertraulichkeit des privaten Schlüssels der Chipkarte	gemSpec_CVC_TSP
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	gemSpec_CVC_TSP
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	gemSpec_CVC_TSP
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_4359-02	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4365-02	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI

Softwareentwicklungsprozesse

Der Hersteller des HSK muss diesen in einer sicheren Entwicklungsumgebung mittels sicherer Software-Entwicklungsprozesse implementieren. Dies ist durch ein Sicherheitsgutachten (Tabelle 13) nachzuweisen.

Alternativ kann der Hersteller dies durch eine positiv abgeschlossene Evaluierung der Entwicklungsumgebung im Rahmen des CC-Verfahrens für einen Einboxkonnektor (Aspekt ALC) nachweisen, wobei von der Prüfstelle die Nutzung der gleichen Entwicklungsumgebung zu bestätigen ist.

Ebenso können bestehende Sicherheitsgutachten nachgenutzt werden, sofern – durch den Gutachter bestätigt – die gleiche Entwicklungsumgebung genutzt wird.

Tabelle 13: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Softwareentwicklungsprozesse

ID	Bezeichnung	Quelle (Referenz)
A_22046	Sichere Software Entwicklungsumgebung	gemF_Highspeed-Konnektor
A_19147	Sicherheitstestplan	gemSpec_DS_Hersteller
A_19148	Sicherheits- und Datenschutzkonzept	gemSpec_DS_Hersteller
A_19150	Umsetzung Sicherheitstestplan	gemSpec_DS_Hersteller
A_19151	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
A_19152	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19153	Sicherheitsrelevanter Softwarearchitektur-Review	gemSpec_DS_Hersteller
A_19154	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
A_19155	Durchführung sicherheitsrelevanter Quellcode-Reviews	gemSpec_DS_Hersteller
A_19156	Durchführung automatisierter Sicherheitstests	gemSpec_DS_Hersteller
A_19157	Dokumentierter Plan zur Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19158	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19159	Dokumentation des sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19160	Änderungs- und Konfigurationsmanagementprozess	gemSpec_DS_Hersteller
A_19161	Verifizierung der Einhaltung sicherheitstechnische Eignung durch Datenschutzbeauftragten	gemSpec_DS_Hersteller

ID	Bezeichnung	Quelle (Referenz)
A_19162	Informationspflicht bei Veröffentlichung neue Produktversion	gemSpec_DS_Hersteller

3.2.5 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 14: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4701-03	TUC_KON_035 „Zertifikatsdienst initialisieren“	gemF_Highspeed-Konnektor
GS-A_4330	Einbringung des Komponentenzertifikats	gemRL_TSL_SP_CP
A_18985-03	ePA-Client: Prüfen der AuthenticationAssertion	gemSpec_Authentisierung_Vers
A_17178	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
A_19163	Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes	gemSpec_DS_Hersteller
A_19164	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller
A_19165	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller
A_23445	Beteiligung der Hersteller am Coordinated Vulnerability Disclosure Programm	gemSpec_DS_Hersteller
GS-A_2330-02	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
GS-A_2350-01	Produktunterstützung der Hersteller	gemSpec_DS_Hersteller
GS-A_2354-01	Produktunterstützung mit geeigneten Sicherheitstechnologien	gemSpec_DS_Hersteller
GS-A_2525-01	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller

ID	Bezeichnung	Quelle (Referenz)
GS-A_4944-01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS-A_4945-01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS-A_4946-01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS-A_4947-01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
AMTS-A_2135	FM AMTS: Verbot der Rückgabe von Implementierungsdetails	gemSpec_FM_AMTS
AMTS-A_2137	FM AMTS: Verbot von personenbezogenen Daten in Fehlermeldungen	gemSpec_FM_AMTS
AMTS-A_2143	FM AMTS: Sicherheitsprotokoll	gemSpec_FM_AMTS
AMTS-A_2146	FM AMTS: Fachmodulprotokoll (Debug)	gemSpec_FM_AMTS
AMTS-A_2149	FM AMTS: Erzeugung von Zugriffsprotokolleinträgen für eGK G2.0	gemSpec_FM_AMTS
AMTS-A_2151	FM AMTS: Format der Zugriffsprotokolleinträge des Fachmoduls AMTS auf der eGK G2.0	gemSpec_FM_AMTS
AMTS-A_2158	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei nicht freigeschalteten Smartcards	gemSpec_FM_AMTS
AMTS-A_2160	FM AMTS: Übergreifende Anforderung – Zugriffsberechtigung auf benötigte Ressourcen	gemSpec_FM_AMTS
AMTS-A_2161	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei fehlender Zugriffsberechtigung	gemSpec_FM_AMTS
AMTS-A_2164	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei nicht erfolgreicher C2C-Prüfung	gemSpec_FM_AMTS
AMTS-A_2172	FM AMTS: Übergreifende Anforderung – Fehlerbehandlung bei eGK-Sperrung	gemSpec_FM_AMTS
AMTS-A_2197	FM AMTS: WriteMP – Fehlerbehandlung bei abweichender Versicherten-ID	gemSpec_FM_AMTS
AMTS-A_2236	FM AMTS: Zusammenfassung mehrerer Protokolleinträge mittels Vorgangsnummer	gemSpec_FM_AMTS

ID	Bezeichnung	Quelle (Referenz)
AMTS-A_2689	FM AMTS: Protokollierung	gemSpec_FM_AMTS
NFDM-A_2100	Sicherheitsprotokoll (SecurityLog)	gemSpec_FM_NFDM
NFDM-A_2104	Übergreifende Konfigurationsparameter	gemSpec_FM_NFDM
VSDM-A_2586	ReadVSD: Protokollierung VSD-Aktualisierung	gemSpec_FM_VSDM
VSDM-A_2591	Fachmodul VSDM: Prüfungsnachweis verschlüsseln	gemSpec_FM_VSDM
VSDM-A_2592	Fachmodul VSDM: Prüfungsnachweis entschlüsseln	gemSpec_FM_VSDM
VSDM-A_2776	Fachmodul VSDM: Schlüssel aus Eingabe ableiten	gemSpec_FM_VSDM
VSDM-A_2777	Fachmodul VSDM: Schlüssel und Prüfungsnachweis mandantenfähig	gemSpec_FM_VSDM
A_14271	FM ePA: ActivateAccount - Terminalanzeige für PIN-Eingaben der Operation	gemSpec_FM_ePA
A_14749	FM ePA: ActivateAccount - Hinterlegen des verschlüsselten Schlüsselmaterials	gemSpec_FM_ePA
A_14829	FM ePA: RequestFacilityAuthorization - Hinterlegen des verschlüsselten Schlüsselmaterials in der Komponente Autorisierung	gemSpec_FM_ePA
A_15137	FM ePA: Übergreifende Anforderung - Unterbindung paralleler Zugriffe auf die eGK - Fehler	gemSpec_FM_ePA
A_16211	FM ePA: Übergreifende Anforderung - Zertifikat auf der eGK nicht prüfbar	gemSpec_FM_ePA
A_16214-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Bestätigung	gemSpec_FM_ePA
A_16215-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Abbruch	gemSpec_FM_ePA
A_16216-01	FM ePA: RequestFacilityAuthorization - Terminalanzeige für PIN-Eingaben der Operation	gemSpec_FM_ePA
A_16218-01	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Nutzerinteraktion	gemSpec_FM_ePA

ID	Bezeichnung	Quelle (Referenz)
A_16219-02	FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Optimierung	gemSpec_FM_ePA
A_17450-01	FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion	gemSpec_FM_ePA
A_17451	FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion - Fehler	gemSpec_FM_ePA
A_17484	FM ePA: Übergreifende Anforderung - Kryptographische Verfahren für Smartcards ab Generation 2.1	gemSpec_FM_ePA
A_17724	FM ePA: Übergreifende Anforderung - Verbot der Rückgabe von Implementierungsdetails	gemSpec_FM_ePA
A_17869	FM ePA: Schlüsselableitung bei Entschlüsselung - Entschlüsselung mit Verschlüsselungsdienst	gemSpec_FM_ePA
A_18009	FM ePA: getDocuments - Entschlüsselung der Dokumente mit Verschlüsselungsdienst	gemSpec_FM_ePA
TIP1-A_3896	Signatur der Update-Informationen durch Konnektorhersteller	gemSpec_KSR
A_18002	TUC_KON_076 „Symmetrisch entschlüsseln“	gemSpec_Kon
A_19738	Optionaler Import von Konfigurationsdaten durch lokalen Administrator	gemSpec_Kon
A_19945	Unterstützte Signaturvarianten bei Komfortsignatur	gemSpec_Kon
A_20478	Zusätzliche Dokumentformate für nonQES-Signatur	gemSpec_Kon
A_22923	XML-Attribute schemaLocation und noNamespaceSchemaLocation nicht auswerten	gemSpec_Kon
TIP1-A_4525	Initialisierung Zugriffsberechtigungsdienst	gemSpec_Kon
TIP1-A_4547	TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	gemSpec_Kon
TIP1-A_4553	Einsichtnahme in und Aktualisierung der Kartenterminaleinträge	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4554	Bearbeitung von Kartenterminaleinträgen	gemSpec_Kon
TIP1-A_4561-02	Terminal-Anzeigen für PIN-Operationen	gemSpec_Kon
TIP1-A_4562	Reaktion auf „Karte entfernt“	gemSpec_Kon
TIP1-A_4568	TUC_KON_019 „PIN ändern“	gemSpec_Kon
TIP1-A_4569-02	TUC_KON_021 „PIN entsperren“	gemSpec_Kon
TIP1-A_4570	TUC_KON_022 „Liefere PIN-Status“	gemSpec_Kon
TIP1-A_4580	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	gemSpec_Kon
TIP1-A_4593	TUC_KON_025 „Initialisierung Kartendienst“	gemSpec_Kon
TIP1-A_4597	Unterstützung von Missbrauchserkennungen	gemSpec_Kon
TIP1-A_4607	Operation GetResourceInformation	gemSpec_Kon
TIP1-A_4614	Missbrauchserkennung Verschlüsselungsdienst	gemSpec_Kon
TIP1-A_4618	TUC_KON_072 „Daten symmetrisch verschlüsseln“	gemSpec_Kon
TIP1-A_4619	TUC_KON_073 „Daten symmetrisch entschlüsseln“	gemSpec_Kon
TIP1-A_4629	Unterstützte Karten QES-Erstellung	gemSpec_Kon
TIP1-A_4645	Zeichen der Jobnummer	gemSpec_Kon
TIP1-A_4646-06	TUC_KON_155 „Dokumente zur Signatur vorbereiten“	gemSpec_Kon
TIP1-A_4669	QES-Stapelsignatur	gemSpec_Kon
TIP1-A_4686	Warnung vor und bei Ablauf der TSL	gemSpec_Kon
TIP1-A_4687	Warnung vor und bei Ablauf des TI-Vertrauensankers	gemSpec_Kon
TIP1-A_4692	Missbrauchserkennung, zu kontrollierende Operationen	gemSpec_Kon
TIP1-A_4707	Betrieb in Test- und Referenzumgebung	gemSpec_Kon
TIP1-A_4708	Protokollierungsfunktion	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4721	TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	gemSpec_Kon
TIP1-A_4792	Explizites Anstoßen der Zeitsynchronisierung	gemSpec_Kon
TIP1-A_4794	Warnung und Übergang in kritischen Betriebszustand bei nichterfolgter Zeitsynchronisierung	gemSpec_Kon
TIP1-A_5033	Missbrauchserkennung Signaturdienst (nonQES)	gemSpec_Kon
TIP1-A_5392	gSMC-K-Verantwortung durch den Hersteller des Konnektors	gemSpec_Kon
TIP1-A_5393	Dokumentation der Konnektorzertifikatszuordnungen	gemSpec_Kon
TIP1-A_5394	Bereitstellen eines Konnektorsperrprozesses	gemSpec_Kon
TIP1-A_5395	Sperrberechtigung der gematik gegenüber Konnektorhersteller	gemSpec_Kon
TIP1-A_5396	Prüfung des Sperrauftrages für Konnektoren	gemSpec_Kon
TIP1-A_5397	Umsetzung von Sperraufträgen für Konnektoren	gemSpec_Kon
TIP1-A_5398	Beschränkung der Sperrberechtigung des Konnektorherstellers	gemSpec_Kon
TIP1-A_5399	Protokollierung der Sperrung von Konnektoren	gemSpec_Kon
TIP1-A_5400	Fortführen des Konnektor-Sperrprozesses	gemSpec_Kon
TIP1-A_5484	Persistente Speicherung von Konfigurationsdaten der Fachmodule	gemSpec_Kon
TIP1-A_5486	TUC_KON_027 „PIN-Schutz ein-/ausschalten“	gemSpec_Kon
TIP1-A_5703	Geschützte Übertragung von Daten zum Kartenpersonalisierer	gemSpec_Kon
TIP1-A_6730	Regelmäßige Aktualisierung der BNetzA-VL	gemSpec_Kon
TIP1-A_6731	Regelmäßige Prüfung der BNetzA-VL	gemSpec_Kon
TIP1-A_7225	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_7255	Anzeige von Fachmodulversionen	gemSpec_Kon
TIP1-A_7281	Authentifizierung des Konnektors durch das Remote-Management-System	gemSpec_Kon
A_15561	AES-NI	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_18465-01	VAU-Protokoll: MTOM/XOP-HTTP-Header-Informationen	gemSpec_Krypt
A_18466-01	VAU-Protokoll: zusätzliche HTTP-Header-Informationen	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_20549	VAU-Protokoll: Einbringen der ursprünglich intendierten Content-Type-Variable	gemSpec_Krypt
A_22457	TLS-Clients, Ciphersuiten bei TLS-Verbindung mit eHealth-KT	gemSpec_Krypt
A_22458	TLS-Algorithmus passend zum Pairing	gemSpec_Krypt
A_23458	Konnektor, Zulässigkeitszeiträume kryptographische Algorithmen	gemSpec_Krypt
A_23511	Konnektor, IOP, Kodierung ECC-Schlüssel, Primärsystem-Verbindungssicherung	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4370	Kryptographische Algorithmen für XML-Dokumente	gemSpec_Krypt
GS-A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
GS-A_4865	Versionierte Liste zulässiger Firmware-Versionen	gemSpec_OM
GS-A_4866	Integritäts- und Authentizitätsschutz der Firmware-Versionsinformationen	gemSpec_OM
GS-A_4867	Übernahme Firmware-Gruppe	gemSpec_OM
GS-A_4868	Aufsteigende Nummerierung der Firmware-Gruppen	gemSpec_OM

ID	Bezeichnung	Quelle (Referenz)
GS-A_4869	Firmware-Gruppe mindestens eine Firmware-Version	gemSpec_OM
GS-A_4870	Wechsel zu jeder Firmware-Version der aktuellen Firmware-Gruppe	gemSpec_OM
GS-A_4871	Upgrade nur auf höhere Firmware-Gruppen-Version	gemSpec_OM
GS-A_4872	Kein Downgrade der Firmware-Gruppe	gemSpec_OM
GS-A_4873	Speicherung der Firmware-Gruppe	gemSpec_OM
GS-A_4874	Firmware-Gruppen-Updates nur über herstellereigenen Update-Mechanismus	gemSpec_OM
GS-A_4941	Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM
GS-A_5018	Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen	gemSpec_OM
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
GS-A_4607	Zuordnung Konnektorinstanz zu verbauter gSMC-K	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
AMTS-A_2114	FM AMTS: WriteConsent – Kein Überschreiben einer vorhandenen Einwilligungsdaten	gemSpec_eGK_Fach_AMTS
AMTS-A_2121	FM AMTS: DeleteConsent – Speicherstruktur EF.AMTS löschen	gemSpec_eGK_Fach_AMTS
TIP1-A_4701-02	TUC_KON_035 „Zertifikatsdienst initialisieren“	gemF_Highspeed-Konnektor
A_16212-03	FM ePA: RequestFacilityAuthorization Version 1.x – Anzeige am Kartenterminal – Anzeigetext	gemSpec_FM_ePA
A_16212-07	FM ePA: RequestFacilityAuthorization Version 2.x – Anzeige am Kartenterminal – Anzeigetext	gemSpec_FM_ePA
TIP1-A_4646-04	ab PTV4: TUC_KON_155 „Dokumente zur Signatur vorbereiten“	gemSpec_Kon

Tabelle 15: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die Herausgabe der gSMC-K

ID	Bezeichnung	Quelle (Referenz)
GS-A_4233	Zertifikatsuspendierung für Kartenzertifikate	gemRL_TSL_SP_CP
TIP1-A_2581	Evaluierung von HSMs	gemSpec_CVC_TSP
GS-A_2355-02	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5559-01	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5560	Entgegennahme und Prüfung von Meldungen der gematik	gemSpec_DS_Anbieter
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_5624-01	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4362-02	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
GS-A_4365-02	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366-02	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4380	Card-to-Server (C2S) Authentisierung und Trusted Channel G2	gemSpec_Krypt
GS-A_4381-01	Schlüssellängen Algorithmus AES	gemSpec_Krypt
GS-A_5021	Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung	gemSpec_Krypt
GS-A_4963	Deaktivierung von Chipkarten nach Gültigkeitsende	gemSpec_PKI
GS-A_4972	Bezug des CV-Zertifikat	gemSpec_PKI
GS-A_4973	Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA	gemSpec_PKI
Card-G2-A_3593	Schlüsselspeicherung	gemSpec_gSMC-K_ObjSys

3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

Da für den Highspeed-Konnektor vorgesehen ist, dass in in die Ablaufumgebung des Betreibers eingebracht wird, werden keine Festlegungen an die Hardware des Konnektors gestellt.

Tabelle 16: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

ID	Bezeichnung	Quelle (Referenz)
	Es liegen keine Festlegungen vor	

4 Produktypspezifische Merkmale

In der konkreten Implementierung des Konnektors hat der Hersteller die Wahl, welche Ausprägungsform er umsetzt.

Die zur Wahl stehenden Ausprägungsformen werden im Folgenden definiert. Im Rahmen der Zulassung muss der Hersteller verbindlich erklären, welche der gelisteten Ausprägungsformen sein Konnektor erfüllt. Im Rahmen der Zulassung muss die Erfüllung der zu diesen Ausprägungsformen gehörenden Festlegungen nachgewiesen werden. Die Zuordnung der Festlegungen zu den Ausprägungsformen erfolgt über Leistungsstufen, die nach dem Bedarf der Leistungserbringenumgebungen geschnitten sind.

4.1 Leistungsstufen

Die Performance des Highspeed-Konnektors wird zwischen Hersteller und Betreiber vereinbart.

4.2 Ausprägungsformen des Konnektors

entfällt

4.3 Optionale Ausprägungen

In diesem Kapitel werden die optionalen Ausprägungen des Zulassungsobjektes Konnektors beschrieben. Festlegungen, die einer Option zugeordnet werden, sind genau dann umzusetzen, wenn das Zulassungsobjekt diese Option unterstützt.

Die Spezifikationen des Konnektors lassen folgende Optionen zu:

- Option IPv6 gemäß Tab_Option IPv6

4.3.1 Option IPv6

Tabelle 17: Tab_Option IPv6

ID	Bezeichnung	Quelle (Referenz)
A_17199	IPv6 - Adressierung der Schnittstelle zum Internet (Option IPv6)	gemSpec_Kon
A_17200	IPv6 - Fragmentierung der IKEv2-Nachrichten (Option IPv6)	gemSpec_Kon
A_17201	IPv6 - Verhalten als IPv6 Router (Option IPv6)	gemSpec_Kon

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4728-01	IPv4 und IPv6 (Option IPv6)	gemSpec_Kon

4.4 Referenzdokumente

In „Performance und Mengengerüst TI-Plattform“ [gemSpec_Perf] werden Referenzdokumente über Bezeichner adressiert. Die Tabelle Tab_Referenzdokumente gibt je Bezeichner die gültige Datei an.

Tabelle 18: Tab_Referenzdokumente

Bezeichner	Datei	Version
TIFF_25MB	TIFF_25MB_V1.0.1.tif	1.0.1
TIFF_1MB	TIFF_1MB_V1.0.1.tif	1.0.1
PDFA_2b_25MB_Bilder_und_Text	PDFA_2b_25MB_Bilder_und_Text_V1.0.1.pdf	1.0.1
PDFA_2b_1MB_Komplex	PDFA_2b_1MB_Komplex_V1.0.1.pdf	1.0.1
TEXT_10KB	TEXT_10KB_V1.0.0.txt	1.0.0
TEXT_100KB	TEXT_100KB_V1.0.0.txt	1.0.0
XML_25MB	XML_25MB_V1.0.0.xml	1.0.0
XML_1MB	XML_1MB_V1.0.0.xml	1.0.0
XML_100KB	XML_100KB_V1.0.0.xml	1.0.0
XML_10KB	XML_10KB_V1.0.0.xml	1.0.0

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit normativen Festlegungen	6
Tabelle 2: Mitgeltende Dokumente	7
Tabelle 3: GitHub Repository-Links	8
Tabelle 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	9
Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"	61
Tabelle 6: Festlegungen zur funktionalen Eignung "Herstellererklärung" zur Herausgabe der gSMC-K	70
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Beschleunigte Sicherheitszertifizierung (BSZ)"	78
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Prüfung durch CC-Prüfstelle"	82
Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"	98
Tabelle 10: Festlegungen zur Herstellererklärung für die Erzeugung herstellerspezifischer Schlüssel und Admin-Schlüssel durch den Hersteller des Konnektors selbst	100
Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitgutachten" spezifisch für die Personalisierung der gSMC-K	100
Tabelle 12: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitgutachten" spezifisch für die Personalisierung des HSM	105
Tabelle 13: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitgutachten" spezifisch für die Softwareentwicklungsprozesse	106

Tabelle 14: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"	107
Tabelle 15: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung" spezifisch für die Herausgabe der gSMC-K	115
Tabelle 16: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	116
Tabelle 17: Tab_Option IPv6	117
Tabelle 18: Tab_Referenzdokumente	118

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung