

**Elektronische Gesundheitskarte und Telematikinfrastuktur**

# **Produkttypsteckbrief**

## ***Prüfvorschrift***

# **KTR-Consumer**

Produkttyp Version: 1.0.1-0  
Produkttyp Status: freigegeben

Version: 1.1.0  
Revision: 166096  
Stand: 02.10.2019  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_KTR-Consumer\_PTV\_1.0.1-0

## gemProdT\_KTR-Consumer

### Historie Produkttypversion

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

| Produkttypversion | Beschreibung der Änderung            | Referenz                           |
|-------------------|--------------------------------------|------------------------------------|
| 1.0.0-0           | Initiale Version auf Dokumentenebene | [gemProdT_KTR-Consumer_PTV1.0.0-0] |
| 1.0.1-0           | Releasestand 3.1.1                   | [gemProdT_KTR-Consumer_PTV1.0.1-0] |

### 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   | 28.06.19 |      | freigegeben                               | gematik    |
| 1.1.0   | 02.10.19 | 2    | Aktualisierung Dokumentenversionen R3.1.2 | gematik    |

---

## Inhaltsverzeichnis

---

|   |           |
|---|-----------|
| <b>1 Einführung .....</b>                                     | <b>4</b>  |
| 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         |
| <b>2 Dokumente .....</b>                                      | <b>6</b>  |
| <b>3 Blattanforderungen .....</b>                             | <b>8</b>  |
| 3.1 Anforderungen zur funktionalen Eignung .....              | 8         |
| 3.1.1 Produkttest/Produktübergreifender Test .....            | 8         |
| 3.1.2 Herstellererklärung funktionale Eignung .....           | 17        |
| 3.2 Anforderungen zur sicherheitstechnischen Eignung .....    | 28        |
| 3.2.1 Produktgutachten .....                                  | 28        |
| 3.2.2 Herstellererklärung sicherheitstechnische Eignung ..... | 32        |
| <b>4 Produkttypspezifische Merkmale .....</b>                 | <b>34</b> |
| <b>5 Anhang – Verzeichnisse .....</b>                         | <b>35</b> |
| 5.1 Abkürzungen .....   | 35        |
| 5.2 Tabellenverzeichnis .....                                 | 35        |
| 5.3 Referenzierte Dokumente .....                             | 35        |

---

## 1 Einführung

---

### 1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen 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 Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

### 1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an Hersteller und Anbieter des Produkttyps KTR-Consumer sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, 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. Dokumentenlandkarte, 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 Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

## 1.5 Methodik

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

**Afo-ID:** Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

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

**Quelle (Referenz):** Verweist auf das Dokument, das die Anforderung definiert.

## 2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

**Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion**

| Dokumenten Kürzel            | Bezeichnung des Dokumentes   | Version |
|------------------------------|--|---------|
| gemSpec_CM_KOMLE             | Spezifikation KOM-LE-Clientmodul   | 1.6.0   |
| gemSpec_DS_Hersteller        | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller                       | 1.1.0   |
| gemSpec_PKI                  | Übergreifende Spezifikation – Spezifikation PKI  | 2.7.0   |
| gemSpec_DM_ePA               | Datenmodell ePA  | 1.3.0   |
| gemKPT_Test                  | Testkonzept der TI   | 2.5.0   |
| gemSpec_Net                  | Übergreifende Spezifikation Netzwerk   | 1.16.0  |
| gemSpec_SGD_ePA              | Spezifikation Schlüsselgenerierungsdienst ePA  | 1.2.0   |
| gemSpec_Krypt                | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.15.0  |
| gemSpec_Basis_KTR_Consumer   | Spezifikation Basis-/KTR-Consumer  | 1.1.0   |
| gemSpec_FM_ePA_KTR_Consumer  | Spezifikation Fachmodul ePA im KTR-Consumer  | 1.1.0   |
| gemSMIME_KOMLE               | S/MIME-Profil Kommunikation Leistungserbringer (KOM-LE)  | 1.2.0   |
| gemSpec_TSL                  | Spezifikation TSL-Dienst   | 1.16.0  |
| gemSpec_HSMProxy             | Übergreifende Spezifikation HSM-Proxy  | 1.0.0   |
| gemSpec_OM                   | Übergreifende Spezifikation Operations und Maintenance   | 1.12.0  |
| gemSpec_Systemprozesse_dezTI | Spezifikation Systemprozesse der dezentralen TI  | 1.2.0   |
| gemSpec_Dokumentenverwaltung | Spezifikation Dokumentenverwaltung ePA   | 1.3.0   |

### Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den

Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

## 3 Blattanforderungen

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

### 3.1 Anforderungen zur funktionalen Eignung

#### 3.1.1 Produkttest/Produktübergreifender Test

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

**Tabelle 2: Anforderungen zur funktionalen Eignung  
"Produkttest/Produktübergreifender Test"**

| Afo-ID  | Afo-Bezeichnung   | Quelle (Referenz)          |
|---------|---|----------------------------|
| A_17298 | Synchronisation mit der Systemzeit der zentralen TI-Plattform                       | gemSpec_Basis_KTR_Consumer |
| A_17299 | Konfigurationsparameter   | gemSpec_Basis_KTR_Consumer |
| A_17302 | Authentisierung gegenüber dem SMTP-Server mit Benutzernamen und Passwort            | gemSpec_Basis_KTR_Consumer |
| A_17337 | Abbrechen des Entschlüsseln, wenn die erforderliche SM-B nicht verfügbar ist        | gemSpec_Basis_KTR_Consumer |
| A_17338 | Abbrechen des Entschlüsseln, wenn Freischaltung der erforderlichen SM-B fehlschlägt | gemSpec_Basis_KTR_Consumer |
| A_17341 | Basis- und KTR-Consumer, LDAPv3-Operationen an der Clientschnittstelle              | gemSpec_Basis_KTR_Consumer |
| A_17343 | Basis- und KTR-Consumer, LDAPv3-Operationen für interne Module                      | gemSpec_Basis_KTR_Consumer |
| A_17400 | NAT-Umsetzung   | gemSpec_Basis_KTR_Consumer |
| A_17401 | Systemprozess<br>PL_TUC_PKI_VERIFY_CERTIFICATE                                      | gemSpec_Basis_KTR_Consumer |
| A_17408 | Basisdienst Zertifikatsdienst   | gemSpec_Basis_KTR_Consumer |



|         |  |                            |
|---------|--|----------------------------|
| A_17411 | Kommunikation mit NET_TI_Offene_FD                   | gemSpec_Basis_KTR_Consumer |
| A_17415 | Kommunikation mit NET_TI_ZENTRAL                     | gemSpec_Basis_KTR_Consumer |
| A_17417 | Einschränkung von nicht genehmigten Traffic          | gemSpec_Basis_KTR_Consumer |
| A_17418 | Drop statt Reject                                    | gemSpec_Basis_KTR_Consumer |
| A_17420 | Eingeschränkte Nutzung von „Ping“                    | gemSpec_Basis_KTR_Consumer |
| A_17424 | Firewall-Protokollierung                             | gemSpec_Basis_KTR_Consumer |
| A_17429 | Basis- und KTR-Consumer, Operation VerifyCertificate | gemSpec_Basis_KTR_Consumer |
| A_17430 | Netzwerk-Routen einrichten                           | gemSpec_Basis_KTR_Consumer |
| A_17466 | Systemprozess<br>PL_TUC_HYBRID_ENCIPHER              | gemSpec_Basis_KTR_Consumer |
| A_17467 | Systemprozess<br>PL_TUC_HYBRID_DECIPHER              | gemSpec_Basis_KTR_Consumer |
| A_17474 | Anzeige IP-Routinginformationen                      | gemSpec_Basis_KTR_Consumer |
| A_17477 | Basisdienst Verschlüsselungsdienst                   | gemSpec_Basis_KTR_Consumer |
| A_17499 | DNS-Forwards des DNS-Servers                         | gemSpec_Basis_KTR_Consumer |
| A_17510 | Basis- und KTR-Consumer, Operation EncryptDocument   | gemSpec_Basis_KTR_Consumer |
| A_17514 | Kommunikation mit<br>NET_TI_Gesicherte_FD            | gemSpec_Basis_KTR_Consumer |
| A_17515 | Basis- und KTR-Consumer, Operation DecryptDocument   | gemSpec_Basis_KTR_Consumer |
| A_17517 | Systemprozess<br>PL_TUC_SIGN_DOCUMENT_nonQES         | gemSpec_Basis_KTR_Consumer |
| A_17518 | Systemprozess<br>PL_TUC_SIGN_HASH_nonQES             | gemSpec_Basis_KTR_Consumer |
| A_17523 | Basisdienst Signaturdienst                           | gemSpec_Basis_KTR_Consumer |
| A_17525 | Basis- und KTR-Consumer, Operation SignDocument      | gemSpec_Basis_KTR_Consumer |
| A_17526 | Basis- und KTR-Consumer, Operation VerifyDocument    | gemSpec_Basis_KTR_Consumer |
| A_17577 | Systemprozess<br>PL_TUC_VERIFY_DOCUMENT_nonQES       | gemSpec_Basis_KTR_Consumer |

|               |  |                            |
|---------------|--|----------------------------|
| A_17578       | Basis- und KTR-Consumer, Operation ExternalAuthenticate                                      | gemSpec_Basis_KTR_Consumer |
| A_17239       | ECC-Migration, Unterstützung verschiedener kryptografischer Verfahren bei der TLS-Verwendung | gemSpec_CM_KOMLE           |
| KOM-LE-A_2004 | Größe einer KOM-LE-Nachricht   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2013 | Unterstützung der Clientteile der Mechanismen PLAIN und LOGIN                                | gemSpec_CM_KOMLE           |
| KOM-LE-A_2016 | Schließen der SMTP-Verbindung mit dem Clientsystem   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2017 | Schließen der SMTP-Verbindung mit dem MTA  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2021 | Verhalten, wenn Nachricht nicht signiert werden kann   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2022 | Verschlüsseln der Nachricht mit den Verschlüsselungszertifikaten C.HCI.ENC bzw. C.HP.ENC     | gemSpec_CM_KOMLE           |
| KOM-LE-A_2024 | Information des Absenders über Empfänger, für die nicht verschlüsselt werden kann            | gemSpec_CM_KOMLE           |
| KOM-LE-A_2025 | Abbruch des Sendens, wenn keine Verschlüsselung möglich                                      | gemSpec_CM_KOMLE           |
| KOM-LE-A_2028 | Entfernen von Empfängern aus dem Header der Nachricht  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2038 | Schließen der POP3-Verbindung mit dem Clientsystem   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2039 | Schließen der POP3-Verbindung mit dem POP3-Server  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2042 | Entschlüsselung einer KOM-LE-SMIME-Nachricht   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2046 | Aufbau der Fehlnachricht bei fehlgeschlagener Entschlüsselung                                | gemSpec_CM_KOMLE           |
| KOM-LE-A_2047 | Fehlertexte bei fehlgeschlagener Entschlüsselung   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2048 | Prüfung der Signatur einer KOM-LE-Nachricht  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2049 | Ergebnis der Signaturprüfung einer KOM-LE-Nachricht  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2050 | Vermerke des Ergebnisses der   | gemSpec_CM_KOMLE           |

|               |   |                  |
|---------------|---|------------------|
|               | Signaturprüfung einer KOM-LE-Nachricht  |                  |
| KOM-LE-A_2057 | Abbrechen des Signierens, wenn keine SM-B verfügbar ist   | gemSpec_CM_KOMLE |
| KOM-LE-A_2058 | Abbrechen des Signierens, wenn Freischaltung der erforderlichen SM-B fehlschlägt                    | gemSpec_CM_KOMLE |
| KOM-LE-A_2066 | Verwendung von TLS für SMTP-Verbindungen mit Clientsystemen   | gemSpec_CM_KOMLE |
| KOM-LE-A_2067 | Verwendung von TLS für POP3-Verbindungen mit Clientsystemen   | gemSpec_CM_KOMLE |
| KOM-LE-A_2074 | Verbindung zu KOM-LE-Fachdiensten immer über TLS  | gemSpec_CM_KOMLE |
| KOM-LE-A_2079 | Protokolldateien für Ablauf, Performance und Fehler   | gemSpec_CM_KOMLE |
| KOM-LE-A_2080 | Keine Protokollierung sensibler Daten   | gemSpec_CM_KOMLE |
| KOM-LE-A_2081 | Format der Protokolldateien   | gemSpec_CM_KOMLE |
| KOM-LE-A_2082 | Zugriff auf Protokolldateien einschränken   | gemSpec_CM_KOMLE |
| KOM-LE-A_2083 | Kopien der Protokolldateien   | gemSpec_CM_KOMLE |
| KOM-LE-A_2084 | Aktivierung und Deaktivierung der Protokollierung von Performanceinformationen                      | gemSpec_CM_KOMLE |
| KOM-LE-A_2085 | Begrenzung des Speicherplatzes für Protokolldateien   | gemSpec_CM_KOMLE |
| KOM-LE-A_2086 | Vorgangsnummer für Protokolleinträge  | gemSpec_CM_KOMLE |
| KOM-LE-A_2087 | Felder zur Protokollierung des Ablaufs  | gemSpec_CM_KOMLE |
| KOM-LE-A_2088 | Felder zur Protokollierung der Performance  | gemSpec_CM_KOMLE |
| KOM-LE-A_2089 | Aktionen zur Protokollierung der Performance  | gemSpec_CM_KOMLE |
| KOM-LE-A_2090 | Felder zur Protokollierung der Fehler   | gemSpec_CM_KOMLE |
| KOM-LE-A_2094 | Skalierbarkeit  | gemSpec_CM_KOMLE |
| KOM-LE-A_2176 | Prüfen auf gültiges ENC-Zertifikat für den Empfänger im RCPT-Kommando                               | gemSpec_CM_KOMLE |
| KOM-LE-A_2178 | Kein Versenden an Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten | gemSpec_CM_KOMLE |

|               |   |                             |
|---------------|---|-----------------------------|
| KOM-LE-A_2179 | Vermerk in der Nachricht bei erfolgreicher Entschlüsselung  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2180 | Struktur des Signaturprüfberichts   | gemSpec_CM_KOMLE            |
| KOM-LE-A_2181 | Authentifizierung von Clientsystemen gegenüber dem Clientmodul  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2192 | Fehlernachricht bei Empfänger mit unterschiedlichen Telematik-IDs in den Verschlüsselungszertifikaten | gemSpec_CM_KOMLE            |
| KOM-LE-A_2225 | Update-Mechanismen  | gemSpec_CM_KOMLE            |
| A_14760       | Nutzungsvorgaben für die Verwendung von XDS-Metadaten   | gemSpec_DM_ePA              |
| A_14762       | Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author           | gemSpec_DM_ePA              |
| A_14763       | Nutzungsvorgabe für DocumentEntry.authorInstitution   | gemSpec_DM_ePA              |
| A_14974       | Nutzungsvorgabe für DocumentEntry.patientId und SubmissionSet.patientId                               | gemSpec_DM_ePA              |
| A_14975       | Verschlüsselung des Dokuments mit dem DocumentKey   | gemSpec_DM_ePA              |
| A_14976       | Verschlüsselung des DocumentKey mit dem RecordKey   | gemSpec_DM_ePA              |
| A_14977       | Dokumentenverschlüsselung gemäß XML Encryption  | gemSpec_DM_ePA              |
| A_17245       | FM ePA KTR-Consumer: Login nach Notwendigkeit   | gemSpec_FM_ePA_KTR_Consumer |
| A_17246       | FM ePA KTR-Consumer: Beenden der Aktensession   | gemSpec_FM_ePA_KTR_Consumer |
| A_17247       | FM ePA KTR-Consumer: Beenden nach Inaktivität   | gemSpec_FM_ePA_KTR_Consumer |
| A_17248       | FM ePA KTR-Consumer: Lokalisierung Komponenten des ePA-Aktensystem                                    | gemSpec_FM_ePA_KTR_Consumer |
| A_17249       | FM ePA KTR-Consumer: Autorisierung - TLS-Verbindung nutzen  | gemSpec_FM_ePA_KTR_Consumer |
| A_17251       | FM ePA KTR-Consumer: Login Aktensession   | gemSpec_FM_ePA_KTR_Consumer |
| A_17252       | FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR -                                    | gemSpec_FM_ePA_KTR_Consumer |

|         |  |                             |
|---------|--|-----------------------------|
|         | Auswahl SMC-KTR  |                             |
| A_17253 | FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR - SAML -Token erstellen       | gemSpec_FM_ePA_KTR_Consumer |
| A_17254 | FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR - Behauptung im SAML-Token    | gemSpec_FM_ePA_KTR_Consumer |
| A_17256 | FM ePA KTR-Consumer: Logout Aktensession   | gemSpec_FM_ePA_KTR_Consumer |
| A_17257 | FM ePA KTR-Consumer: Logout - Aktenkontext schliessen  | gemSpec_FM_ePA_KTR_Consumer |
| A_17259 | FM ePA KTR-Consumer: Dokumente einstellen  | gemSpec_FM_ePA_KTR_Consumer |
| A_17261 | FM ePA KTR-Consumer: Dokumente einstellen - Metadaten  | gemSpec_FM_ePA_KTR_Consumer |
| A_17262 | FM ePA KTR-Consumer: Dokumente einstellen - Dokument verschlüsseln                             | gemSpec_FM_ePA_KTR_Consumer |
| A_17264 | FM ePA KTR-Consumer: Dokumente einstellen - Dokumentenset in Dokumentenverwaltung hochladen    | gemSpec_FM_ePA_KTR_Consumer |
| A_17265 | FM ePA KTR-Consumer: IHE XDS-Transaktion [ITI-41]  | gemSpec_FM_ePA_KTR_Consumer |
| A_17266 | FM ePA KTR-Consumer: IHE XDS-Transaktion [ITI-41] - Unterstützung MTOM/XOP                     | gemSpec_FM_ePA_KTR_Consumer |
| A_17281 | FM ePA KTR-Consumer: Autorisierung - Aufbau TLS-Verbindung                                     | gemSpec_FM_ePA_KTR_Consumer |
| A_17282 | FM ePA KTR-Consumer: Dokumentenverwaltung - TLS-Verbindung nutzen                              | gemSpec_FM_ePA_KTR_Consumer |
| A_17283 | FM ePA KTR-Consumer: Dokumentenverwaltung - Aufbau TLS-Verbindung                              | gemSpec_FM_ePA_KTR_Consumer |
| A_17284 | FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Erweiterung des sicheren Verbindungsprotokolls | gemSpec_FM_ePA_KTR_Consumer |
| A_17285 | FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Fehler beim Verbindungsaufbau                  | gemSpec_FM_ePA_KTR_Consumer |
| A_17286 | FM ePA KTR-Consumer: Login - Autorisierung - Schlüsselmaterial laden                           | gemSpec_FM_ePA_KTR_Consumer |

|           |  |                             |
|-----------|--|-----------------------------|
| A_17318   | FM ePA KTR-Consumer: Login - Aktenkontext öffnen - Operation OpenContext     | gemSpec_FM_ePA_KTR_Consumer |
| A_17323   | FM ePA KTR-Consumer: Dokumente einstellen - Upload verschlüsselter Dokumente | gemSpec_FM_ePA_KTR_Consumer |
| A_17782   | FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Serverzertifikat prüfen      | gemSpec_FM_ePA_KTR_Consumer |
| A_17955   | FM ePA KTR-Consumer: ePA-Dienst  | gemSpec_FM_ePA_KTR_Consumer |
| A_17958   | FM ePA KTR-Consumer: Operation PutDocuments- RecordIdentifier bilden         | gemSpec_FM_ePA_KTR_Consumer |
| A_17959   | FM ePA KTR-Consumer: Operation PutDocuments - SMC-KTR auswählen              | gemSpec_FM_ePA_KTR_Consumer |
| A_17960   | FM ePA KTR-Consumer: Operation Logout  | gemSpec_FM_ePA_KTR_Consumer |
| A_17961   | FM ePA KTR-Consumer: Operation Logout - Anwendungsfall starten               | gemSpec_FM_ePA_KTR_Consumer |
| A_17962   | FM ePA KTR-Consumer: Operation PutDocuments                                  | gemSpec_FM_ePA_KTR_Consumer |
| A_17963   | FM ePA KTR-Consumer: Operation PutDocuments - Anwendungsfall starten         | gemSpec_FM_ePA_KTR_Consumer |
| A_17970   | FM ePA KTR-Consumer: Operation PutDocuments - Metadaten SubmissionSet        | gemSpec_FM_ePA_KTR_Consumer |
| A_17971   | FM ePA KTR-Consumer: Operation PutDocuments - Document                       | gemSpec_FM_ePA_KTR_Consumer |
| A_17972   | FM ePA KTR-Consumer: Operation PutDocuments - Metadaten Document Entry       | gemSpec_FM_ePA_KTR_Consumer |
| A_18185   | FM ePA KTR-Consumer: Prüfung TI-Zertifikate (SGD-Zertifikate)                | gemSpec_FM_ePA_KTR_Consumer |
| GS-A_4759 | IPv4-Adressen Produkttyp zum SZZP  | gemSpec_Net                 |
| GS-A_4832 | Path MTU Discovery und ICMP Response   | gemSpec_Net                 |
| A_15237   | Transport Fehlermeldungen als gematik-SOAP-Fault- SOAP 1.2                   | gemSpec_OM                  |
| GS-A_3702 | Inhalt der Selbstauskunft von Produkten außer Karten                         | gemSpec_OM                  |
| GS-A_3796 | Transport Fehlermeldungen als gematik-                                       | gemSpec_OM                  |

|           |   |             |
|-----------|---|-------------|
|           | SOAP-Fault - SOAP 1.1   |             |
| GS-A_3801 | Abbildung von Fehlern auf Transportprotokollebene   | gemSpec_OM  |
| GS-A_3856 | Struktur der Fehlermeldungen  | gemSpec_OM  |
| GS-A_4547 | Generische Fehlermeldungen  | gemSpec_OM  |
| GS-A_5025 | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM  |
| A_17688   | Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)  | gemSpec_PKI |
| A_17689   | Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)  | gemSpec_PKI |
| A_17690   | Nutzung der Hash-Datei für TSL (ECC-Migration)  | gemSpec_PKI |
| A_17700   | TSL-Auswertung ServiceTypenidentifizier "unspecified"   | gemSpec_PKI |
| A_17820   | Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)  | gemSpec_PKI |
| A_17821   | Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)   | 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 |
| 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 | TUC_PKI_018: Zertifikatsprüfung in der TI                   | gemSpec_PKI     |
| GS-A_4653 | TUC_PKI_002: Gültigkeitsprüfung des Zertifikats             | gemSpec_PKI     |
| GS-A_4654 | TUC_PKI_003: CA-Zertifikat finden                           | gemSpec_PKI     |
| GS-A_4655 | 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 | TUC_PKI_006: OCSP-Abfrage                                   | gemSpec_PKI     |
| GS-A_4660 | TUC_PKI_009: Rollenermittlung                               | gemSpec_PKI     |
| GS-A_4661 | 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 | TUC_PKI_007: Prüfung Zertifikatstyp                         | 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_4943 | Alter der OCSP-Responses für eGK-Zertifikate                | gemSpec_PKI     |
| GS-A_4957 | 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     |
| GS-A_5336 | Zertifikatsprüfung nach Ablauf TSL-Graceperiod              | gemSpec_PKI     |
| A_17893   | Maximale Größe der JSON-Requests und -Responses             | gemSpec_SGD_ePA |
| A_17925   | SGD-Client, Parallele Anfrage SGD1 und SGD2                 | gemSpec_SGD_ePA |



|             |   |             |
|-------------|---|-------------|
| TIP1-A_5120 | Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen | gemSpec_TSL |
|-------------|---|-------------|

### 3.1.2 Herstellererklärung funktionale Eignung

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

**Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"**

| Afo-ID      | Afo-Bezeichnung  | Quelle (Referenz) |
|-------------|--|-------------------|
| A_17317     | Zugang zum KTR-Consumer bzw. Basis-Consumer                          | 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                        | gemKPT_Test       |
| TIP1-A_4191 | Keine Echtdaten in RU und TU   | gemKPT_Test       |
| TIP1-A_4929 | Nachweis über Qualität der Zufallszahlen                             | gemKPT_Test       |
| TIP1-A_6088 | Unterstützung bei Fehlernachstellung                                 | gemKPT_Test       |
| 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 | Testdokumentation gemäß Vorlagen                                     | gemKPT_Test       |
| TIP1-A_6527 | Testkarten   | gemKPT_Test       |
| TIP1-A_6529 | Produkttypen: Mindestumfang der Interoperabilitätsprüfung            | gemKPT_Test       |
| 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:                                 | gemKPT_Test       |

|               | Aufgaben der TDI                                      |                |
|---------------|---|----------------|
| TIP1-A_6772   | Partnerprodukte bei Interoperabilitätstests           | gemKPT_Test    |
| TIP1-A_7330   | Tracedaten von echten Außenschnittstellen             | gemKPT_Test    |
| TIP1-A_7331   | Bereitstellung von Tracedaten an Außenschnittstelle   | gemKPT_Test    |
| 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    |
| KOM-LE-A_2095 | Reihenfolge Signatur und Verschlüsselung              | gemSMIME_KOMLE |
| KOM-LE-A_2096 | Signatur und Verschlüsselung entsprechend S/MIME V3.2 | gemSMIME_KOMLE |
| KOM-LE-A_2097 | Verschlüsselter Body                                  | gemSMIME_KOMLE |
| KOM-LE-A_2098 | Header der äußeren Nachricht                          | gemSMIME_KOMLE |
| KOM-LE-A_2099 | Header-Element X-KOM-LE-Version                       | gemSMIME_KOMLE |
| KOM-LE-A_2100 | Wert Header-Element X-KOM-LE-Version                  | gemSMIME_KOMLE |
| KOM-LE-A_2101 | Neues message-id Element                              | gemSMIME_KOMLE |
| KOM-LE-A_2102 | Wert subject Header-Element                           | gemSMIME_KOMLE |
| KOM-LE-A_2103 | Opak-Signatur   | gemSMIME_KOMLE |
| KOM-LE-A_2104 | Typ S/MIME-Verschlüsselung                            | gemSMIME_KOMLE |
| KOM-LE-A_2106 | AuthenticatedEnvelopedData ohne originatorInfo        | gemSMIME_KOMLE |
| KOM-LE-A_2107 | AuthenticatedEnvelopedData mit unauthAttrs            | gemSMIME_KOMLE |
| KOM-LE-A_2108 | Schlüsselverwaltungsalgorithmus                       | gemSMIME_KOMLE |
| KOM-LE-A_2109 | Zertifikatsidentifizierung bei keyTransRecipientInfo  | gemSMIME_KOMLE |
| KOM-LE-A_2111 | RecipientInfo Element für Sender                      | gemSMIME_KOMLE |

|               |  |                            |
|---------------|--|----------------------------|
| KOM-LE-A_2112 | Inhalt von authEncryptedContentInfo                                  | gemSMIME_KOMLE             |
| KOM-LE-A_2114 | Attribut recipient-emails  | gemSMIME_KOMLE             |
| KOM-LE-A_2115 | Referenzierte Zertifikate in RecipientEmail                          | gemSMIME_KOMLE             |
| KOM-LE-A_2116 | E-Mail-Adresse des Zertifikatsinhabers                               | gemSMIME_KOMLE             |
| KOM-LE-A_2117 | Zertifikatsidentifikation über Aussteller und Seriennummer           | gemSMIME_KOMLE             |
| KOM-LE-A_2118 | Keine crls in signed-data  | gemSMIME_KOMLE             |
| KOM-LE-A_2119 | Signed-data muss certificates enthalten                              | gemSMIME_KOMLE             |
| KOM-LE-A_2121 | Signierte Daten im Element eContent                                  | gemSMIME_KOMLE             |
| KOM-LE-A_2122 | Signaturzertifikat im Element Zertifikate                            | gemSMIME_KOMLE             |
| KOM-LE-A_2123 | Genau ein signerInfo Element   | gemSMIME_KOMLE             |
| KOM-LE-A_2124 | Inhalt Element sid aus Unterzeichnerinformationen                    | gemSMIME_KOMLE             |
| KOM-LE-A_2125 | Aussteller und Seriennummer entsprechend Signaturzertifikat          | gemSMIME_KOMLE             |
| KOM-LE-A_2126 | Unterzeichnerinformationen ohne unsignedAttrs                        | gemSMIME_KOMLE             |
| KOM-LE-A_2127 | Unterzeichnerinformationen mit signiertem Attribut recipient-emails  | gemSMIME_KOMLE             |
| KOM-LE-A_2128 | Zertifikate für Verschlüsselung                                      | gemSMIME_KOMLE             |
| KOM-LE-A_2129 | Signaturzertifikat   | gemSMIME_KOMLE             |
| A_17300       | Initialer SMTP-Dialog  | gemSpec_Basis_KTR_Consumer |
| A_17301       | Verbindungsaufbau mit dem SMTP-Servers                               | gemSpec_Basis_KTR_Consumer |
| A_17303       | Ergebnis des Verbindungsaufbaus mit dem SMTP-Server                  | gemSpec_Basis_KTR_Consumer |
| A_17305       | Verwenden von PL_TUC_SIGN_DOCUMENT_nonQES und PL_TUC_HYBRID_ENCIPHER | gemSpec_Basis_KTR_Consumer |
| A_17327       | Signieren der Nachricht mit dem Schlüssel Prk.HCI.OSIG               | gemSpec_Basis_KTR_Consumer |
| A_17328       | POP3-Dialog zur Authentifizierung                                    | gemSpec_Basis_KTR_Consumer |
| A_17329       | Verbindungsaufbau mit dem POP3-                                      | gemSpec_Basis_KTR_Consumer |

|         |  |                            |
|---------|--|----------------------------|
|         | Servers  |                            |
| A_17330 | Authentifizierung gegenüber POP3-Server mit Benutzernamen und Passwort | gemSpec_Basis_KTR_Consumer |
| A_17331 | Ergebnis des Verbindungsaufbaus mit dem POP3-Server                    | gemSpec_Basis_KTR_Consumer |
| A_17333 | E-Mail-Adresse des den Abholvorgang auslösenden Nutzers                | gemSpec_Basis_KTR_Consumer |
| A_17396 | Verhalten als IPv4-Router  | gemSpec_Basis_KTR_Consumer |
| A_17397 | IP-Pakete mit Source Route Option                                      | gemSpec_Basis_KTR_Consumer |
| A_17405 | Nur IPv4. IPv6 nur hardwareseitig vorbereitet                          | gemSpec_Basis_KTR_Consumer |
| A_17406 | Kein dynamisches Routing   | gemSpec_Basis_KTR_Consumer |
| A_17419 | Abwehr von IP-Spoofing, DoS/DDoS-Angriffe und Martian Packets          | gemSpec_Basis_KTR_Consumer |
| A_17421 | Einschränkungen der IP-Protokolle                                      | gemSpec_Basis_KTR_Consumer |
| A_17423 | Firewall Restart   | gemSpec_Basis_KTR_Consumer |
| A_17425 | Reagiere auf LAN_IP_Changed  | gemSpec_Basis_KTR_Consumer |
| A_17426 | Reagiere auf WAN_IP_Changed  | gemSpec_Basis_KTR_Consumer |
| A_17485 | Maximale Zeitabweichung  | gemSpec_Basis_KTR_Consumer |
| A_17498 | Grundlagen des Namensdienstes  | gemSpec_Basis_KTR_Consumer |
| A_17500 | DNS Stub-Resolver  | gemSpec_Basis_KTR_Consumer |
| A_17502 | TUC_CON_362 „Liste der Dienste abrufen“                                | gemSpec_Basis_KTR_Consumer |
| A_17503 | Prüfung von TLS-Server-Zertifikaten                                    | gemSpec_Basis_KTR_Consumer |
| A_17504 | Verwenden von PL_TUC_VERIFY_DOCUMENT_nonQES und PL_TUC_HYBRID_DECIPHER | gemSpec_Basis_KTR_Consumer |
| A_17509 | Basisanwendung Namensdienst  | gemSpec_Basis_KTR_Consumer |
| A_17512 | Initialisierung „Namensdienst und Dienstlokalisierung“                 | gemSpec_Basis_KTR_Consumer |
| A_17513 | Konfigurationsparameter Namensdienst und Dienstlokalisierung           | gemSpec_Basis_KTR_Consumer |
| A_17574 | Infrastruktur Konfiguration aktualisieren                              | gemSpec_Basis_KTR_Consumer |

|               |   |                            |
|---------------|---|----------------------------|
| A_17576       | KSR lokalisieren  | gemSpec_Basis_KTR_Consumer |
| A_17598       | Qualität des HSM  | gemSpec_Basis_KTR_Consumer |
| A_17599       | Personalisierung des HSM  | gemSpec_Basis_KTR_Consumer |
| A_17712       | Zusätzlich alternative Schnittstellentechnologien   | gemSpec_Basis_KTR_Consumer |
| KOM-LE-A_2003 | Unterstützung von E-Mail-Clients  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2005 | Keine persistente Speicherung von Nachrichten   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2006 | Einzuhaltende Standards beim Senden und Empfangen   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2007 | SMTP Begrüßung  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2009 | Unterstützung der Serverteile der Mechanismen PLAIN und LOGIN                                 | gemSpec_CM_KOMLE           |
| KOM-LE-A_2014 | Authentifizierung gegenüber MTA mit anderen Mechanismen als PLAIN und LOGIN                   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2018 | Weiterleitung von SMTP-Meldungen und Antwortcodes   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2019 | Signatur und Verschlüsselung entsprechend KOM-LE-S/MIME-Profil                                | gemSpec_CM_KOMLE           |
| KOM-LE-A_2020 | Signieren der Nachricht mit dem Schlüssel Prk.HCI.OSIG  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2023 | Verschlüsselungszertifikate aus dem Verzeichnisdienst   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2026 | Cachen von Verschlüsselungszertifikaten   | gemSpec_CM_KOMLE           |
| KOM-LE-A_2027 | Befüllung des recipient-emails Attributs  | gemSpec_CM_KOMLE           |
| KOM-LE-A_2029 | Aufbereitung einer vom Clientsystem erhaltenen KOM-LE-S/MIME-Nachricht                        | gemSpec_CM_KOMLE           |
| KOM-LE-A_2031 | Unterstützung der Serverteile der Mechanismen USER/PASS und SASL PLAIN                        | gemSpec_CM_KOMLE           |
| KOM-LE-A_2035 | Unterstützung der Clientteile der Mechanismen USER/PASS und SASL PLAIN                        | gemSpec_CM_KOMLE           |
| KOM-LE-A_2036 | Authentifizierung gegenüber POP3-Server mit anderen Mechanismen als USER/PASS oder SASL PLAIN | gemSpec_CM_KOMLE           |

|               |   |                             |
|---------------|---|-----------------------------|
| KOM-LE-A_2040 | Übermittlung von POP3-Kommandos und -Meldungen nach erfolgreicher Authentifizierung                   | gemSpec_CM_KOMLE            |
| KOM-LE-A_2041 | Setzen des Parameters <N> des TOP-Kommandos auf Null  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2043 | Beachtung des recipient-emails Attributs bei der Entschlüsselung                                      | gemSpec_CM_KOMLE            |
| KOM-LE-A_2064 | Verwendung von X.509-Identitäten bei der TLS-Authentifizierung  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2193 | Verpacken des verschlüsselten CMS-Objektes  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2300 | Import des Schlüsselmateriail für TLS-Verbindungen  | gemSpec_CM_KOMLE            |
| KOM-LE-A_2301 | Individuelles Schlüsselmateriail für TLS-Verbindungen   | gemSpec_CM_KOMLE            |
| A_17258       | FM ePA KTR-Consumer: Logout - Session-Daten löschen   | gemSpec_FM_ePA_KTR_Consumer |
| A_17838       | FM ePA KTR-Consumer: Autorisierung - Symmetrische Schlüssel für Akten- und Kontextschlüssel ermitteln | gemSpec_FM_ePA_KTR_Consumer |
| A_17996       | FM ePA KTR-Consumer: Autorisierung - Aufrufe zur Schlüsselableitung parallelisieren                   | gemSpec_FM_ePA_KTR_Consumer |
| A_17997       | FM ePA KTR-Consumer: Autorisierung - Akten- und Kontextschlüssel entschlüsseln                        | gemSpec_FM_ePA_KTR_Consumer |
| 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       | VAU-Protokoll: ECDH durchführen   | gemSpec_Krypt               |
| A_16883       | VAU-Protokoll: Aufbau VAUClientHello-Nachricht  | gemSpec_Krypt               |
| A_16884       | VAU-Protokoll: Nachrichtentypen und HTTP-Content-Type   | gemSpec_Krypt               |
| A_16897       | VAU-Protokoll: Versand der VAUClientHello-Nachricht   | gemSpec_Krypt               |

|         |   |               |
|---------|---|---------------|
| A_16900 | VAU-Protokoll: Client, Behandlung von Fehlnachrichten   | gemSpec_Krypt |
| A_16903 | VAU-Protokoll: Client, Prüfung des VAUClientHelloDataHash-Werts (aus VAUServerHelloData)        | gemSpec_Krypt |
| A_16941 | VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData                              | gemSpec_Krypt |
| A_16943 | VAU-Protokoll: Schlüsselableitung (HKDF)  | gemSpec_Krypt |
| A_16945 | VAU-Protokoll: Client, verschlüsselte Kommunikation (1)   | gemSpec_Krypt |
| A_16957 | VAU-Protokoll: Client, verschlüsselte Kommunikation (2)   | gemSpec_Krypt |
| A_16958 | VAU-Protokoll: Client, Neuinitiiieren einer Schlüsselaushandlung                                | gemSpec_Krypt |
| A_17069 | VAU-Protokoll: Client Zählerüberlauf  | gemSpec_Krypt |
| A_17070 | VAU-Protokoll: Aufbau der VAUClientSigFin-Nachricht   | gemSpec_Krypt |
| 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_17124 | TLS-Verbindungen (ECC-Migration)  | gemSpec_Krypt |
| A_17205 | Signatur der TSL: Signieren und Prüfen (ECC-Migration)  | gemSpec_Krypt |
| A_17220 | Verschlüsselung binärer Daten (ECIES) (ECC-Migration)   | gemSpec_Krypt |
| A_17221 | XML-Verschlüsselung (ECIES) (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 Chiffren (innerhalb von ePA)              | gemSpec_Krypt |
| A_18464   | TLS-Verbindungen, nicht Version 1.1                                      | gemSpec_Krypt |
| A_18465   | VAU-Protokoll: MTOM/XOP-HTTP-Header-Informationen                        | gemSpec_Krypt |
| A_18466   | VAU-Protokoll: zusätzliche optionale HTTP-Header-Informationen           | gemSpec_Krypt |
| GS-A_4385 | TLS-Verbindungen, Version 1.2  | gemSpec_Krypt |
| GS-A_3834 | DNS-Protokoll, Nameserver-Implementierungen                              | gemSpec_Net   |
| GS-A_3842 | DNS, Verwendung von iterativen queries zwischen Nameservern              | gemSpec_Net   |
| GS-A_4009 | Übertragungstechnologie auf OSI-Schicht LAN                              | gemSpec_Net   |
| GS-A_4010 | Standards für IPv6   | gemSpec_Net   |
| GS-A_4011 | Unterstützung des Dual-Stack Mode  | gemSpec_Net   |
| GS-A_4012 | Leistungsanforderungen an den Dual-Stack Mode                            | gemSpec_Net   |
| GS-A_4053 | Ingress und Egress Filtering   | gemSpec_Net   |
| GS-A_4054 | Paketfilter Default Deny   | gemSpec_Net   |
| GS-A_4805 | Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz    | gemSpec_Net   |
| GS-A_4831 | Standards für IPv4   | gemSpec_Net   |
| GS-A_4884 | Erlaubte ICMP-Types  | 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  | gemSpec_OM    |



|           |   |                 |
|-----------|---|-----------------|
|           | Testumgebung  |                 |
| 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_4542 | Spezifikationsgrundlage für Produkte  | gemSpec_OM      |
| GS-A_5018 | Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen                                  | gemSpec_OM      |
| GS-A_5033 | Betriebsdokumentation der zentralen Produkte der TI-Plattform und anwendungsspezifischen Diensten | gemSpec_OM      |
| GS-A_5038 | Festlegungen zur Vergabe einer Produktversion   | gemSpec_OM      |
| GS-A_5039 | 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_4640 | Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung                 | gemSpec_PKI     |
| 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_17924 | Anfragen an das SGD-HSM (Client)   | gemSpec_SGD_ePA              |
| A_17930 | interoperables Austauschformat Schlüsselableitungsfunktionalität ePA         | gemSpec_SGD_ePA              |
| A_18005 | SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars | gemSpec_SGD_ePA              |
| A_18024 | SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel                                  | gemSpec_SGD_ePA              |
| A_18025 | 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 | SGD-Client, Auswertung der Anfrage KeyDerivation                             | gemSpec_SGD_ePA              |
| A_18032 | SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar                           | gemSpec_SGD_ePA              |
| A_18249 | Groß- und Kleinschreibung von Daten in Hexadezimalform                       | gemSpec_SGD_ePA              |
| A_18250 | keine führenden Nullen bei Punktkoordinaten                                  | gemSpec_SGD_ePA              |
| A_14970 | Leistung zum symmetrischen Verschlüsseln                                     | gemSpec_Systemprozesse_dezTI |
| A_14971 | Aufrufparameter zum symmetrischen Verschlüsseln                              | gemSpec_Systemprozesse_dezTI |
| A_14972 | Ablauf des symmetrischen Verschlüsseln eines Dokuments                       | gemSpec_Systemprozesse_dezTI |
| A_17376 | Leistung der nonQES Dokumenten-Signatur                                      | gemSpec_Systemprozesse_dezTI |
| A_17377 | Aufrufparameter der nonQES Dokumenten-Signatur                               | gemSpec_Systemprozesse_dezTI |
| A_17380 | Ergebnis der nonQES Dokumenten-Signatur                                      | gemSpec_Systemprozesse_dezTI |
| A_17431 | Leistung zum Verbindungsaufbau zum VZD                                       | gemSpec_Systemprozesse_dezTI |
| A_17432 | Leistung zur Abfrage des VZD   | gemSpec_Systemprozesse_dezTI |

|             |   |                              |
|-------------|---|------------------------------|
| A_17445     | Aufbau der Verbindung zum VZD                             | gemSpec_Systemprozesse_dezTI |
| A_17446     | Leistung zur Verbindungstrennung zum VZD                  | gemSpec_Systemprozesse_dezTI |
| A_17447     | Leistung zum Abbrechen einer Verzeichnisabfrage           | gemSpec_Systemprozesse_dezTI |
| A_17448     | Aufrufparameter der Verzeichnisabfrage                    | gemSpec_Systemprozesse_dezTI |
| A_17449     | Ergebnis der Verzeichnisabfrage                           | gemSpec_Systemprozesse_dezTI |
| A_17465     | Trennen der Verbindung zum VZD                            | gemSpec_Systemprozesse_dezTI |
| A_17468     | Abbrechen einer Verzeichnisabfrage                        | gemSpec_Systemprozesse_dezTI |
| A_17559     | Leistung zur Prüfung der nonQES Dokumentensignatur        | gemSpec_Systemprozesse_dezTI |
| A_17561     | Aufrufparameter zur Prüfung der nonQES Dokumentensignatur | gemSpec_Systemprozesse_dezTI |
| A_17562     | Ablauf der Prüfung der nonQES Dokumentensignatur          | gemSpec_Systemprozesse_dezTI |
| A_18072     | Ablauf der Zertifikatsprüfung in der TI                   | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6927 | Leistung zum Lesen einer Datei                            | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6928 | Aufrufparameter für das Lesen einer Datei                 | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6929 | Optionale Parameter für das Lesen einer Datei             | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6930 | Ergebnis des Lesens des Inhalts einer Datei               | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6977 | Auflösen von URI in IP-Adresse                            | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6978 | Synchronisierung mit Zeitdienst                           | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6979 | Leistung der nonQES-Signatur                              | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6980 | Aufrufparameter der nonQES-Signatur                       | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6981 | Ergebnis der nonQES-Signatur                              | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6982 | Leistung zum hybriden Verschlüsseln                       | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6983 | Aufrufparameter zum hybriden Verschlüsseln                | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6984 | Ablauf der hybriden Verschlüsselung eines Dokuments       | gemSpec_Systemprozesse_dezTI |

|             |   |                              |
|-------------|---|------------------------------|
| TIP1-A_6985 | Leistung zum hybriden Entschlüsseln                 | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6986 | Aufrufparameter zum hybriden Entschlüsseln          | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6987 | Ablauf der hybriden Entschlüsselung eines Dokuments | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6991 | Leistung zur Prüfung eines Zertifikats in der TI    | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6992 | Aufrufparameter der Zertifikatsprüfung in der TI    | gemSpec_Systemprozesse_dezTI |
| TIP1-A_6993 | Ergebnis der Zertifikatsprüfung in der TI           | gemSpec_Systemprozesse_dezTI |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 Produktgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL\_PruefSichEig]. Das entsprechende Produktgutachten ist der gematik vorzulegen.

**Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten"**

| Afo-ID  | Afo-Bezeichnung   | Quelle (Referenz)           |
|---------|---|-----------------------------|
| A_14975 | Verschlüsselung des Dokuments mit dem DocumentKey   | gemSpec_DM_ePA              |
| A_14976 | Verschlüsselung des DocumentKey mit dem RecordKey   | gemSpec_DM_ePA              |
| A_17250 | FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Umsetzung sicherer Kanal                              | gemSpec_FM_ePA_KTR_Consumer |
| A_17255 | FM ePA KTR-Consumer: Löschen der AuthenticationAssertion  | gemSpec_FM_ePA_KTR_Consumer |
| A_17258 | FM ePA KTR-Consumer: Logout - Session-Daten löschen   | gemSpec_FM_ePA_KTR_Consumer |
| A_17263 | FM ePA KTR-Consumer: Dokumente einstellen - Dokumentenschlüssel löschen                               | gemSpec_FM_ePA_KTR_Consumer |
| A_17280 | FM ePA KTR-Consumer: Umsetzung der Aktensession in einer Vertrauenswürdigem Ausführungsumgebung (VAU) | gemSpec_FM_ePA_KTR_Consumer |
| A_17281 | FM ePA KTR-Consumer: Autorisierung -  | gemSpec_FM_ePA_KTR_Consumer |

|         |   |                             |
|---------|---|-----------------------------|
|         | Aufbau TLS-Verbindung   |                             |
| A_17283 | FM ePA KTR-Consumer: Dokumentenverwaltung - Aufbau TLS-Verbindung   | gemSpec_FM_ePA_KTR_Consumer |
| A_17323 | FM ePA KTR-Consumer: Dokumente einstellen - Upload verschlüsselter Dokumente                                      | gemSpec_FM_ePA_KTR_Consumer |
| A_17346 | FM ePA KTR-Consumer: Verarbeitungskontext der VAU   | gemSpec_FM_ePA_KTR_Consumer |
| A_17347 | FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Keine persistente Speicherung von Akten- und Kontextschlüssel | gemSpec_FM_ePA_KTR_Consumer |
| A_17348 | FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Akten- und Kontextschlüssel verlassen VAU nie                 | gemSpec_FM_ePA_KTR_Consumer |
| A_17350 | FM ePA KTR-Consumer: Isolation der VAU von Datenverarbeitungsprozessen des Anbieters                              | gemSpec_FM_ePA_KTR_Consumer |
| A_17351 | FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Software der VAU  | gemSpec_FM_ePA_KTR_Consumer |
| A_17352 | FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Hardware der VAU  | gemSpec_FM_ePA_KTR_Consumer |
| A_17353 | FM ePA KTR-Consumer: Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU                                | gemSpec_FM_ePA_KTR_Consumer |
| A_17356 | FM ePA KTR-Consumer: Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes                   | gemSpec_FM_ePA_KTR_Consumer |
| A_17357 | FM ePA KTR-Consumer: Autorisierung - TLS-Verbindung in VAU terminieren  | gemSpec_FM_ePA_KTR_Consumer |
| A_17358 | FM ePA KTR-Consumer: Dokumentenverwaltung - TLS-Verbindung in VAU terminieren                                     | gemSpec_FM_ePA_KTR_Consumer |
| A_17385 | FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Nutzung sicherer Kanal  | gemSpec_FM_ePA_KTR_Consumer |
| A_17838 | FM ePA KTR-Consumer: Autorisierung - Symmetrische Schlüssel für Akten- und Kontextschlüssel ermitteln             | gemSpec_FM_ePA_KTR_Consumer |
| A_17997 | FM ePA KTR-Consumer: Autorisierung - Akten- und Kontextschlüssel entschlüsseln                                    | gemSpec_FM_ePA_KTR_Consumer |

|         |  |                             |
|---------|--|-----------------------------|
| A_17999 | FM ePA KTR-Consumer:<br>informationstechnische Trennung von<br>Aktensessions                   | gemSpec_FM_ePA_KTR_Consumer |
| A_17714 | HSM-Proxy - Eindeutige Referenz der<br>kryptografischen Identität                              | gemSpec_HSMPProxy           |
| A_17715 | HSM-Proxy - Identifikation und<br>Authentisierung des Eigentümers des<br>privaten Schlüssels   | gemSpec_HSMPProxy           |
| A_17716 | HSM-Proxy - Vertrauliche und<br>integritätsgeschützte Kommunikation                            | gemSpec_HSMPProxy           |
| A_15549 | VAU-Client: Kommunikation zwischen VAU-<br>Client und VAU                                      | gemSpec_Krypt               |
| A_15705 | Vorgaben Aktenschlüssel (RecordKey) und<br>Kontextschlüssel (ContextKey)                       | gemSpec_Krypt               |
| A_16849 | VAU-Protokoll: Aktionen bei Protokollabbruch   | gemSpec_Krypt               |
| A_16852 | VAU-Protokoll: ECDH durchführen  | gemSpec_Krypt               |
| A_16883 | VAU-Protokoll: Aufbau VAUClientHello-<br>Nachricht   | gemSpec_Krypt               |
| A_16884 | VAU-Protokoll: Nachrichtentypen und HTTP-<br>Content-Type                                      | gemSpec_Krypt               |
| A_16897 | VAU-Protokoll: Versand der VAUClientHello-<br>Nachricht  | gemSpec_Krypt               |
| A_16900 | VAU-Protokoll: Client, Behandlung von<br>Fehlernachrichten                                     | gemSpec_Krypt               |
| A_16903 | VAU-Protokoll: Client, Prüfung des<br>VAUClientHelloDataHash-Werts (aus<br>VAUServerHelloData) | gemSpec_Krypt               |
| A_16941 | VAU-Protokoll: Client, Prüfung der Signatur<br>der VAUServerHelloData                          | gemSpec_Krypt               |
| A_16943 | VAU-Protokoll: Schlüsselableitung (HKDF)   | gemSpec_Krypt               |
| A_16945 | VAU-Protokoll: Client, verschlüsselte<br>Kommunikation (1)                                     | gemSpec_Krypt               |
| A_16957 | VAU-Protokoll: Client, verschlüsselte<br>Kommunikation (2)                                     | gemSpec_Krypt               |
| A_17069 | VAU-Protokoll: Client Zählerüberlauf   | gemSpec_Krypt               |
| A_17070 | VAU-Protokoll: Aufbau der VAUClientSigFin-<br>Nachricht  | gemSpec_Krypt               |

|           |  |                 |
|-----------|--|-----------------|
| 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_17872   | Ver- und Entschlüsselung der Akten und Kontextschlüssel<br>(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   |
| A_18464   | TLS-Verbindungen, nicht Version 1.1  | gemSpec_Krypt   |
| A_18465   | VAU-Protokoll: MTOM/XOP-HTTP-Header-Informationen  | gemSpec_Krypt   |
| A_18466   | VAU-Protokoll: zusätzliche optionale HTTP-Header-Informationen                                     | gemSpec_Krypt   |
| A_18467   | TLS-Verbindungen, Version 1.3  | gemSpec_Krypt   |
| GS-A_4385 | TLS-Verbindungen, Version 1.2  | gemSpec_Krypt   |
| GS-A_4641 | Initiale Einbringung TI-Vertrauensanker  | gemSpec_PKI     |
| GS-A_4748 | Initiale Einbringung TSL-Datei   | gemSpec_PKI     |
| 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_17924 | Anfragen an das SGD-HSM (Client)   | gemSpec_SGD_ePA |
| A_17930 | interoperables Austauschformat Schlüsselableitungsfunktionalität ePA         | gemSpec_SGD_ePA |
| A_18005 | SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars | gemSpec_SGD_ePA |
| A_18024 | SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel                                  | gemSpec_SGD_ePA |
| A_18025 | 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 | SGD-Client, Auswertung der Anfrage KeyDerivation                             | gemSpec_SGD_ePA |
| A_18032 | SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar                           | gemSpec_SGD_ePA |

### 3.2.2 Herstellererklärung sicherheitstechnische Eignung

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

**Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

| Afo-ID        | Afo-Bezeichnung  | Quelle (Referenz)          |
|---------------|--|----------------------------|
| A_17306       | Vorgehen bei Signatur und Verschlüsselung einer KOM-LE Nachricht | gemSpec_Basis_KTR_Consumer |
| KOM-LE-A_2045 | Entschlüsselung nur mit Schlüsseln des abholenden Nutzers        | gemSpec_CM_KOMLE           |
| KOM-LE-A_2048 | Prüfung der Signatur einer KOM-LE-Nachricht                      | gemSpec_CM_KOMLE           |



|               |   |                       |
|---------------|---|-----------------------|
| KOM-LE-A_2050 | Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht   | gemSpec_CM_KOMLE      |
| KOM-LE-A_2065 | Schutz des Schlüsselspeichers für TLS-Verbindungen  | gemSpec_CM_KOMLE      |
| KOM-LE-A_2182 | Verwendung des vom KOM-LE-Anbieter zur Verfügung gestellten Zertifikats für die clientseitige TLS-Authentifizierung | gemSpec_CM_KOMLE      |
| A_17178       | Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken  | gemSpec_DS_Hersteller |
| A_17179       | Auslieferung aktueller zusätzlicher Softwarekomponenten   | 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_2524-01  | Produktunterstützung: Nutzung des Problem-Management-Prozesses  | gemSpec_DS_Hersteller |
| GS-A_2525-01  | Hersteller: Schließen von Schwachstellen  | gemSpec_DS_Hersteller |
| 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 |
| A_17124       | TLS-Verbindungen (ECC-Migration)  | gemSpec_Krypt         |
| A_17205       | Signatur der TSL: Signieren und Prüfen (ECC-Migration)  | gemSpec_Krypt         |

---

## 4 Produktypspezifische Merkmale

---

Es liegen keine optionalen Ausprägungen des Produktyps vor.

## 5 Anhang – Verzeichnisse

### 5.1 Abkürzungen

| Kürzel | Erläuterung                 |
|--------|-----------------------------|
| Afo-ID | Anforderungs-Identifikation |

### 5.2 Tabellenverzeichnis

|  |    |
|--|----|
| Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion.....                             | 6  |
| Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" ..... | 8  |
| Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellereklärung" .....                     | 17 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten" .....             | 28 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" .....           | 32 |

### 5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| [Quelle]             | Herausgeber: Titel, Version                            |
|----------------------|--|
| [gemRL_PruefSichEig] | gematik: Richtlinie zur Prüfung der Sicherheitseignung |