

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Produkttypsteckbrief**

## ***Prüfvorschrift***

# **Fachdienst KOM-LE**

Produkttyp Version: 1.6.0-0  
Produkttyp Status: freigegeben

Version: 1.0.0  
Revision: 354852  
Stand: 06.04.2021  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_FD\_KOMLE\_PTV\_1.6.0-0

---

## Historie Produkttypversion und Produkttypsteckbrief

---

### 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             | Initiale Version                                | [gemProdT_FD_KOMLE_PTV1.0.0]   |
| 1.1.0             | Anforderung ergänzt                             | [gemProdT_FD_KOMLE_PTV1.1.0]   |
| 1.2.0             | Weitere Anforderungen ergänzt, ORS1-Release 1.4 | [gemProdT_FD_KOMLE_PTV1.2.0]   |
| 1.2.1-0           | Anpassung auf Releasestand 2.1.2                | [gemProdT_FD_KOMLE_PTV1.2.1-0] |
| 1.2.2-0           | Anpassung auf Releasestand 2.1.2-1              | [gemProdT_FD_KOMLE_PTV1.2.2-0] |
| 1.3.0-0           | Anpassung auf Releasestand 3.1.0                | [gemProdT_FD_KOMLE_PTV1.3.0-0] |
| 1.3.1-0           | Anpassung auf Releasestand 3.1.2                | [gemProdT_FD_KOMLE_PTV1.3.1-0] |
| 1.3.2-0           | Anpassung auf Releasestand 3.1.3                | [gemProdT_FD_KOMLE_PTV1.3.2-0] |
| 1.5.0-0           | Anpassung auf Releasestand 4.0.0                | [gemProdT_FD_KOMLE_PTV1.5.0-0] |
| 1.5.0-1           | Anpassung auf Releasestand 4.0.1 Hotfix 1       | [gemProdT_FD_KOMLE_PTV1.5.0-1] |
| 1.5.0-2           | Anpassung auf Releasestand 4.0.1 Hotfix 2       | [gemProdT_FD_KOMLE_PTV1.5.0-2] |
| 1.5.1-0           | Anpassung auf Releasestand 4.0.2                | [gemProdT_FD_KOMLE_PTV1.5.1-0] |
| 1.6.0-0           | Anpassung auf Releasestand KIM 1.5.1            | [gemProdT_FD_KOMLE_PTV1.6.0-0] |

### 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   | 06.04.21 |      | freigegeben                            | gematik    |

---

## Inhaltsverzeichnis

---

|  |           |
|--|-----------|
| <b>1 Einführung .....</b>  | <b>5</b>  |
| 1.1 Zielsetzung und Einordnung des Dokumentes .....                                  | 5         |
| 1.2 Zielgruppe .....   | 5         |
| 1.3 Geltungsbereich .....  | 5         |
| 1.4 Abgrenzung des Dokumentes .....  | 5         |
| 1.5 Methodik .....   | 6         |
| <b>2 Dokumente .....</b>   | <b>7</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 .....                                  | 14        |
| 3.2 Anforderungen zur sicherheitstechnischen Eignung .....                           | 17        |
| 3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie .... | 17        |
| 3.2.2 CC-Evaluierung .....   | 17        |
| 3.2.3 Sicherheitsgutachten .....   | 17        |
| 3.2.4 Herstellererklärung sicherheitstechnische Eignung .....                        | 19        |
| 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung .....    | 21        |
| <b>4 Produkttypspezifische Merkmale .....</b>  | <b>22</b> |
| <b>5 Anhang A – Verzeichnisse .....</b>  | <b>23</b> |
| 5.1 Abkürzungen .....  | 23        |
| 5.2 Tabellenverzeichnis .....  | 23        |
| 5.3 Referenzierte Dokumente.....   | 23        |

---

## **1 Einführung**

---

### **1.1 Zielsetzung und Einordnung des Dokumentes**

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an die Herstellung des Bestätigungsobjektes Fachdienst KOM-LE oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Bestätigungen durch die gematik.

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 für das Bestätigungsobjekt Fachdienst KOM-LE richtet sich an Fachdienst KOM-LE-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 Bestätigungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- akkreditierten Materialprüflaboren
- Auditoren

Die Anforderungen beziehen sich auf den Hersteller des Bestätigungsobjektes Fachdienst KOM-LE.

### **1.3 Geltungsbereich**

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Bestätigungsverfahren 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 Bestätigungsverfahren für das Bestätigungsobjekt Fachdienst KOM-LE sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und

Durchführung von Bestätigungsverfahren 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 wider, 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 das Bestätigungsobjekt Fachdienst KOM-LE normativen Anforderungen.

**Tabelle 1: Dokumente mit Anforderungen zu dem Bestätigungsobjekt**

| Dokumenten Kürzel   | Bezeichnung des Dokumentes   | Version              |
|---------------------|--|----------------------|
| gemSpec_VZD         | Spezifikation Verzeichnisdienst  | 1.1 <del>23</del> .0 |
| gemSpec_Net         | Übergreifende Spezifikation Netzwerk   | 1.20. <del>01</del>  |
| gemKPT_Test         | Testkonzept der TI   | 2.8.0                |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter                         | 1.3.0                |
| gemSpec_Krypt       | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.19.0               |
| gemSpec_OM          | Übergreifende Spezifikation Operations und Maintenance   | 1.14.0               |
| gemSpec_SST_LD_BD   | Spezifikation Logdaten und Betriebsdatenerfassung  | 1.2.0                |
| gemSpec_Perf        | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform                              | 2.12. <del>42</del>  |
| gemSpec_ServiceMon  | Spezifikation Service Monitoring   | 1.5.0                |
| gemRL_TSL_SP_CP     | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL             | 2.7.0                |
| gemSpec_PKI         | Übergreifende Spezifikation – Spezifikation PKI  | 2.10.2               |
| gemSpec_TSL         | Spezifikation TSL-Dienst   | 1.19.0               |
| gemSpec_FD_KOMLE    | Spezifikation Fachdienst KOM-LE  | 1.1 <del>23</del> .0 |

Die Bestätigungsbedingungen für das Bestätigungsobjekt Fachdienst KOM-LE werden im Dokument [gemZul\_Best\_KOM-LE] im Fachportal der gematik im Abschnitt Zulassung veröffentlicht.

### 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 das Bestätigungsobjekt Fachdienst KOM-LE normativen Anforderungen, die für die Entwicklung und den Betrieb von Produkten des Bestätigungsobjektes Fachdienst KOM-LE notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der 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 Bestätigungsobjektes Fachdienst KOM-LE verzeichnet, deren Umsetzung im Zuge von Bestätigungstests durch die gematik geprüft wird.

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

| Afo-ID                     | Afo-Bezeichnung  | Quelle (Referenz)                |
|----------------------------|--|----------------------------------|
| A_17240                    | ECC-Migration, Unterstützung verschiedener kryptografischer Verfahren bei der TLS-Verwendung       | gemSpec_FD_KOMLE                 |
| <a href="#">A_19375-02</a> | <a href="#">KAS – Implementierung der Schnittstelle</a>  | <a href="#">gemSpec_FD_KOMLE</a> |
| A_19377                    | KAS – TLS-gesicherte Verbindung  | gemSpec_FD_KOMLE                 |
| A_19378                    | KAS – Dokumentengröße prüfen   | gemSpec_FD_KOMLE                 |
| A_19379                    | KAS – Dokumentenzugriff  | gemSpec_FD_KOMLE                 |
| A_19380                    | KAS – Erzeugung Freigabelink   | gemSpec_FD_KOMLE                 |
| A_19381                    | KAS – Freigabelink Transportsicherheit   | gemSpec_FD_KOMLE                 |
| A_19519-01                 | KAS – Maximale Mailgröße bereitstellen   | gemSpec_FD_KOMLE                 |
| A_19524                    | Verwaltung Resource Records Typs für Service Discovery, KIM  | gemSpec_FD_KOMLE                 |
| A_19533                    | Verwaltung Resource Records FQDN, KIM  | gemSpec_FD_KOMLE                 |
| <a href="#">A_19542-01</a> | <a href="#">Schnittstelle für den Download</a>   | <a href="#">gemSpec_FD_KOMLE</a> |
| A_19591                    | Eintrag Clientmodul-Version in VZD, Account Manager  | gemSpec_FD_KOMLE                 |
| <a href="#">A_20063-01</a> | <a href="#">Account Manager - Implementierung der Schnittstelle</a>                                | <a href="#">gemSpec_FD_KOMLE</a> |
| A_20064                    | Account Manager - TLS-gesicherte Verbindung  | gemSpec_FD_KOMLE                 |
| A_20212                    | Verwendung der Schnittstelle I_Directory_Application_Maintenance, Lokalisierung Verzeichniseintrag | gemSpec_FD_KOMLE                 |
| <a href="#">A_20651-02</a> | <a href="#">Empfang von Fehlermeldungen des Clientmodules</a>                                      | <a href="#">gemSpec_FD_KOMLE</a> |
| <a href="#">A_20771-01</a> | <a href="#">Generierung von Fehlermeldungen am Fachdienst</a>                                      | <a href="#">gemSpec_FD_KOMLE</a> |
| <a href="#">A_21376</a>    | <a href="#">Eintrag der KOM-LE-Fachdaten in den VZD</a>  | <a href="#">gemSpec_FD_KOMLE</a> |
| <a href="#">A_21377</a>    | <a href="#">Generierung eines One-Time-Passwortes</a>  | <a href="#">gemSpec_FD_KOMLE</a> |
| <a href="#">A_21378</a>    | <a href="#">Wechsel der Telematik-ID</a>   | <a href="#">gemSpec_FD_KOMLE</a> |



| Afo-ID           | Afo-Bezeichnung  | Quelle (Referenz) |
|------------------|--|-------------------|
| A_21379          | Aktualisierung der Telematik-ID im Verzeichnisdienst               | gemSpec_FD_KOMLE  |
| A_21383          | Authentifizierung mit Benutzername und Passwort                    | gemSpec_FD_KOMLE  |
| A_21385          | Änderung des initialen Passwortes                                  | gemSpec_FD_KOMLE  |
| A_21386          | KAS - HTTP-Basic-Authentifizierung                                 | gemSpec_FD_KOMLE  |
| A_21531          | Eindeutige Zuordnung von KOM-LE Adressen zu VZD-Einträgen          | gemSpec_FD_KOMLE  |
| KOM-LE-A_2130    | Generieren einer Zustellbestätigung                                | gemSpec_FD_KOMLE  |
| KOM-LE-A_2131-01 | Fehlernachricht bei fehlerhafter E-Mail-Adresse                    | gemSpec_FD_KOMLE  |
| KOM-LE-A_2132-01 | Identifikation der Originalnachricht                               | gemSpec_FD_KOMLE  |
| KOM-LE-A_2134    | Aktionen bei Fehlerzuständen                                       | gemSpec_FD_KOMLE  |
| KOM-LE-A_2135-01 | Protokollierung von Vorgängen                                      | gemSpec_FD_KOMLE  |
| KOM-LE-A_2136    | Protokollierung außerhalb gesetzlicher und vertraglicher Pflichten | gemSpec_FD_KOMLE  |
| KOM-LE-A_2139-01 | Konfiguration Fachdienst   | gemSpec_FD_KOMLE  |
| KOM-LE-A_2140    | Schnittstelle I_Message_Service                                    | gemSpec_FD_KOMLE  |
| KOM-LE-A_2141    | Technische Umsetzung der Schnittstelle I_Message_Service           | gemSpec_FD_KOMLE  |
| KOM-LE-A_2142    | Ports der Schnittstelle I_Message_Service                          | gemSpec_FD_KOMLE  |
| KOM-LE-A_2145    | Validierung der TSL  | gemSpec_FD_KOMLE  |
| KOM-LE-A_2146-03 | Verarbeitung von Nachrichten entsprechend S/MIME-Profil            | gemSpec_FD_KOMLE  |
| KOM-LE-A_2147-01 | Generierung von Zustellbestätigungen                               | gemSpec_FD_KOMLE  |
| KOM-LE-A_2149    | Kein Empfang von Nachrichten bei deregistriertem Konto             | gemSpec_FD_KOMLE  |
| KOM-LE-A_2150    | Kein Versenden von Nachrichten bei deregistriertem Konto           | gemSpec_FD_KOMLE  |
| KOM-LE-A_2154-01 | Versand von Löschbenachrichtigungen                                | gemSpec_FD_KOMLE  |
| KOM-LE-A_2155-01 | Nicht abgeholte Nachrichten nach der Deregistrierung               | gemSpec_FD_KOMLE  |
| KOM-LE-A_2158    | Protokollieren von Registrierung und Deregistrierung               | gemSpec_FD_KOMLE  |
| KOM-LE-A_2159-01 | Verwendung der Schnittstelle I_Directory_Application_Maintenance   | gemSpec_FD_KOMLE  |
| KOM-LE-A_2160    | Kommunikation mit dem Verzeichnisdienst über TLS                   | gemSpec_FD_KOMLE  |

| Afo-ID               | Afo-Bezeichnung  | Quelle (Referenz) |
|----------------------|--|-------------------|
| KOM-LE-A_216<br>1    | Benutzername der KOM-LE-Teilnehmers  | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>2    | Übermittlung der Passwörter zum Fachdienst   | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>3-01 | Vorgaben zur Minimum-Qualität des Passwortes   | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>5    | Möglichkeit der Änderung des Passwortes  | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>6    | Keine Änderung oder Löschung des Passwortes durch Dritte   | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>7-03 | Sperrung des Accounts  | gemSpec_FD_KOMLE  |
| KOM-LE-A_216<br>9    | Authentifizierungsdaten beim Versenden und Empfangen von Nachrichten                                 | gemSpec_FD_KOMLE  |
| KOM-LE-A_218<br>6    | Verwendung des C.FD.TLS-S Server-Zertifikats bei der TLS-Authentifizierung mit dem Clientmodul       | gemSpec_FD_KOMLE  |
| KOM-LE-A_218<br>7-02 | Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager                       | gemSpec_FD_KOMLE  |
| KOM-LE-A_218<br>9    | Verwendung des C.FD.TLS-C Client-Zertifikats bei der TLS-Authentifizierung mit dem Verzeichnisdienst | gemSpec_FD_KOMLE  |
| KOM-LE-A_222<br>3-01 | Unterstützung Autoreply für Abwesenheitsnotiz  | gemSpec_FD_KOMLE  |
| KOM-LE-A_222<br>4-01 | Einstellen von Abwesenheitsnotizen   | gemSpec_FD_KOMLE  |
| KOM-LE-A_222<br>8-01 | Ausschließliche Akzeptanz von TLS-Client-Zertifikaten von KOM-LE Clientmodulen                       | gemSpec_FD_KOMLE  |
| KOM-LE-A_223<br>1    | Schnittstellen der TI-Plattform  | gemSpec_FD_KOMLE  |
| KOM-LE-A_227<br>7    | Versenden von Abwesenheitsnotizen ohne Signatur und Verschlüsselung                                  | gemSpec_FD_KOMLE  |
| KOM-LE-A_227<br>8-01 | Aufbau Autoreply für Abwesenheitsnotiz   | gemSpec_FD_KOMLE  |
| KOM-LE-A_230<br>4    | Information an Nutzer zur bcc-Funktionalität   | gemSpec_FD_KOMLE  |
| KOM-LE-A_230<br>5    | Mehrere KOM-LE Postfächer für einen KOM-LE-Teilnehmer  | gemSpec_FD_KOMLE  |
| A_21275-01           | TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake                           | gemSpec_Krypt     |
| GS-A_4384            | TLS-Verbindungen   | gemSpec_Krypt     |
| GS-A_4385            | TLS-Verbindungen, Version 1.2  | gemSpec_Krypt     |
| GS-A_3832            | DNS-Protokoll, Resolver-Implementierungen  | gemSpec_Net       |
| GS-A_3842            | DNS, Verwendung von iterativen queries zwischen Nameservern  | gemSpec_Net       |
| GS-A_3931            | DNSSEC-Protokoll, Nameserver-Implementierungen   | gemSpec_Net       |
| GS-A_3932            | Abfrage der in der Topologie am nächsten stehenden Nameservers                                       | gemSpec_Net       |

| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz) |
|--------------|---|-------------------|
| GS-A_3934    | NTP-Client-Implementierungen, Protokoll NTPv4   | gemSpec_Net       |
| GS-A_3937    | NTP-Client-Implementierungen, Association Mode und Polling Intervall  | gemSpec_Net       |
| GS-A_4036    | Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen   | gemSpec_Net       |
| GS-A_4763    | Einsatz von Hochverfügbarkeitsprotokollen   | gemSpec_Net       |
| GS-A_4817    | Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI                              | gemSpec_Net       |
| GS-A_4819    | Schnittstelle I_NTP_Time_Information, Nutzung durch fachanwendungsspezifische Dienste   | gemSpec_Net       |
| GS-A_4832    | Path MTU Discovery und ICMP Response  | gemSpec_Net       |
| GS-A_3695    | Grundlegender Aufbau Versionsnummern  | 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        |
| GS-A_3801    | Abbildung von Fehlern auf Transportprotokollebene   | gemSpec_OM        |
| GS-A_3816    | Festlegung sicherheitsrelevanter Fehler   | gemSpec_OM        |
| GS-A_3856-02 | Struktur der Fehlermeldungen  | gemSpec_OM        |
| GS-A_4543    | Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten   | gemSpec_OM        |
| GS-A_4545    | Kurzform der Selbstauskunft für zentrale Produkttypen der TI-Plattform und fachanwendungsspezifische Dienste an die Störungsampel                         | gemSpec_OM        |
| GS-A_4547    | Generische Fehlermeldungen  | gemSpec_OM        |
| GS-A_4864    | Logging-Vorgaben nach dem Übergang zum Produktivbetrieb   | gemSpec_OM        |
| GS-A_5025    | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM        |
| GS-A_5252    | Generische Fehlermeldungen außerhalb von WebServices  | 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 ServiceTypeldentifizier "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       |

| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz) |
|--------------|---|-------------------|
| 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_4652-01 | 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_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_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       |
| GS-A_5336    | Zertifikatsprüfung nach Ablauf TSL-Graceperiod                                | gemSpec_PKI       |
| A_17671      | Performance - Rohdaten-Performance-Berichte - Format des Performance-Berichts | gemSpec_Perf      |
| A_17678      | Performance - Rohdaten-Performance-Berichte - Übermittlung                    | gemSpec_Perf      |
| A_17679      | Performance - Rohdaten-Performance-Berichte - Berichtsintervall               | gemSpec_Perf      |
| A_17755      | Performance - Rohdaten-Performance-Berichte - Name der Berichte               | gemSpec_Perf      |
| A_17756      | Performance - Rohdaten-Performance-Berichte - Korrektheit                     | gemSpec_Perf      |
| A_17757-01   | Performance - Rohdaten-Performance-Lieferung - zu liefernde Dateien           | gemSpec_Perf      |
| A_17758      | Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung         | gemSpec_Perf      |
| A_20127      | Performance - KOM-LE-Fachdienst – Spitzenlastvorgaben für den KAS             | gemSpec_Perf      |
| A_20130      | Performance - KOM-LE-Fachdienst - TLS Kanal KAS                               | gemSpec_Perf      |
| A_20132      | Performance - KOM-LE-Fachdienst - Spitzenlastvorgaben TU                      | gemSpec_Perf      |

| Afo-ID           | Afo-Bezeichnung   | Quelle (Referenz)  |
|------------------|---|--------------------|
| A_20134          | Performance - KOM-LE-Fachdienst - Robustheit gegenüber Lastspitzen  | gemSpec_Perf       |
| A_20136          | Performance - Erfassung von Rohdaten - KOM-LE-Fachdienst  | gemSpec_Perf       |
| GS-A_5138-01     | Performance – KOM-LE-Fachdienst – Bearbeitungszeit unter Last   | gemSpec_Perf       |
| A_17416-01       | Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste                          | gemSpec_SST_LD_BD  |
| A_17733-01       | Schnittstelle Betriebsdatenerfassung Datei-Upload   | gemSpec_SST_LD_BD  |
| A_15166          | Nutzer der Schnittstelle I_Monitoring_Update, Zertifikatsprüfung  | gemSpec_ServiceMon |
| TIP1-A_7117      | Service Monitoring und Client, I_Monitoring_Update, Webservice  | gemSpec_ServiceMon |
| TIP1-A_7120      | Service Monitoring und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittlung | gemSpec_ServiceMon |
| TIP1-A_7126      | Nutzer des Service Monitorings I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung                                     | gemSpec_ServiceMon |
| TIP1-A_7128      | Nutzer des Service Monitorings I_Monitoring_Update, maximale HTTP-Nachrichtenlänge  | gemSpec_ServiceMon |
| 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        |
| TIP1-A_5591      | FAD, TUC_VZD_0006 “add_Directory_FA-Attributes (SOAP)”  | gemSpec_VZD        |
| TIP1-A_5594      | FAD, TUC_VZD_0007 “add_Directory_FA-Attributes (LDAPv3)”  | gemSpec_VZD        |
| TIP1-A_5596      | FAD, TUC_VZD_0008 “delete_Directory_FA-Attributes (SOAP)”   | gemSpec_VZD        |
| TIP1-A_5598      | FAD, TUC_VZD_0009 “delete_Directory_FA-Attributes (LDAPv3)”   | gemSpec_VZD        |
| TIP1-A_5600      | FAD, TUC_VZD_0010 “modify_Directory_FA-Attributes (SOAP)”   | gemSpec_VZD        |
| TIP1-A_5603      | FAD, TUC_VZD_0011 “modify_Directory_FA-Attributes (LDAPv3)”   | gemSpec_VZD        |
| A_19375-01       | <del>KAS – Implementierung der Schnittstelle</del>  | gemSpec_FD_KOMLE   |
| A_19542          | <del>Schnittstelle für den Download</del>   | gemSpec_FD_KOMLE   |
| A_20063          | <del>Account Manager – Implementierung der Schnittstelle</del>  | gemSpec_FD_KOMLE   |
| A_20651-01       | <del>Empfang von Fehlermeldungen des Clientmoduls</del>   | gemSpec_FD_KOMLE   |
| A_20771          | <del>Generierung von Fehlermeldungen am Fachdienst</del>  | gemSpec_FD_KOMLE   |
| KOM-LE-A_2139    | <del>Konfiguration Fachdienst</del>   | gemSpec_FD_KOMLE   |
| KOM-LE-A_2167-02 | <del>Sperrung des Accounts</del>  | gemSpec_FD_KOMLE   |
| KOM-LE-A_2187-01 | <del>Authentifizierung des KOM-LE-Teilnehmers über AUT-Zertifikat am AccountManager</del>   | gemSpec_FD_KOMLE   |
| KOM-LE-A_2223    | <del>Unterstützung Autoreply für Abwesenheitsnotiz</del>  | gemSpec_FD_KOMLE   |

| Afo-ID        | Afo-Bezeichnung                        | Quelle (Referenz) |
|---------------|--|-------------------|
| KOM-LE-A_2224 | Einstellen von Abwesenheitsnotizen     | gemSpec_FD_KOMLE  |
| KOM-LE-A_2278 | Aufbau Autoreply für Abwesenheitsnotiz | gemSpec_FD_KOMLE  |

### 3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Bestätigungsobjektes Fachdienst KOM-LE verzeichnet, deren Erfüllung der Hersteller bzw. der Anbieter durch eine Herstellererklärung belegt.

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

| Afo-ID         | Afo-Bezeichnung   | Quelle (Referenz) |
|----------------|---|-------------------|
| A_18892        | Durchführung von gematik-Testfällen (EvT) beim Fachdienst KOM-LE          | gemKPT_Test       |
| A_20065        | Nutzung der Dokumententemplates der gematik                               | gemKPT_Test       |
| GS-A_2162      | Kryptographisches Material in Entwicklungs- und Testumgebungen            | gemKPT_Test       |
| TIP1-A_4191    | Keine Echtdateien 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_6088    | Unterstützung bei Fehlernachstellung                                      | gemKPT_Test       |
| TIP1-A_6093    | Ausprägung der Referenzobjekte  | gemKPT_Test       |
| TIP1-A_6517-01 | Eigenverantwortlicher Test: TBI   | 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_6524-01 | Testdokumentation gemäß Vorlagen  | gemKPT_Test       |
| TIP1-A_6526    | Produkttypen: Bereitstellung  | 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: 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       |

| Afo-ID           | Afo-Bezeichnung   | Quelle (Referenz) |
|------------------|---|-------------------|
| TIP1-A_7335      | Bereitstellung der Testdokumentation  | gemKPT_Test       |
| TIP1-A_7358      | Qualität des Produktmusters   | gemKPT_Test       |
| A_19383          | KAS – Keine Kopien von gelöschten Daten                                       | gemSpec_FD_KOMLE  |
| A_19384          | KAS – Sicher gegen Datenverlust   | gemSpec_FD_KOMLE  |
| A_19385          | KAS – Löschen von Ressource   | gemSpec_FD_KOMLE  |
| A_20772          | I_AccountManager_Service Zeichensatz Fachdienst                               | gemSpec_FD_KOMLE  |
| A_21455          | Festlegung des Localparts einer KIM-Adresse                                   | gemSpec_FD_KOMLE  |
| A_21456          | Festlegung des Domainparts einer KIM-Adresse                                  | gemSpec_FD_KOMLE  |
| KOM-LE-A_2138    | Auskunfts-fähigkeit über den Systemzustand                                    | gemSpec_FD_KOMLE  |
| KOM-LE-A_2143    | Aufbau der TLS-Verbindung   | gemSpec_FD_KOMLE  |
| KOM-LE-A_2144    | Schritte beim Aufbau der TLS-Verbindung                                       | gemSpec_FD_KOMLE  |
| KOM-LE-A_2148-01 | Herleitung der authorizationID beim PLAIN Authentifizierungsverfahren         | gemSpec_FD_KOMLE  |
| KOM-LE-A_2152    | Unterstützung des POP3-Kommandos UIDL   | gemSpec_FD_KOMLE  |
| KOM-LE-A_2171    | Skalierbarkeit KOM-LE-Fachdienst  | gemSpec_FD_KOMLE  |
| KOM-LE-A_2226    | Zuordnung TLS-Client-Zertifikat für Clientmodul                               | gemSpec_FD_KOMLE  |
| KOM-LE-A_2227    | Zuordnung TLS-Server-Zertifikat für Clientmodul                               | gemSpec_FD_KOMLE  |
| A_17124          | TLS-Verbindungen (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_17322          | TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration) | gemSpec_Krypt     |
| A_17360          | XML-Signaturen (Dokumente) (ECC-Migration)                                    | gemSpec_Krypt     |
| A_17775          | TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)                     | gemSpec_Krypt     |
| GS-A_4388        | DNSSEC-Kontext  | gemSpec_Krypt     |
| GS-A_5526        | TLS-Renegotiation-Indication-Extension  | gemSpec_Krypt     |
| GS-A_5542        | TLS-Verbindungen (fatal Alert bei Abbrüchen)                                  | gemSpec_Krypt     |
| GS-A_3824        | FQDN von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform    | gemSpec_Net       |
| GS-A_4009        | Übertragungstechnologie auf OSI-Schicht LAN                                   | gemSpec_Net       |
| GS-A_4013        | Nutzung von UDP/TCP-Portbereichen   | gemSpec_Net       |
| GS-A_4018        | Dokumentation UDP/TCP-Portbereiche Anbieter                                   | gemSpec_Net       |
| GS-A_4024        | Nutzung IP-Adressbereiche   | gemSpec_Net       |
| GS-A_4027        | Reporting IP-Adressbereiche   | gemSpec_Net       |



| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz)  |
|--------------|---|--------------------|
| GS-A_4033    | Statisches Routing TI-Übergabepunkte  | gemSpec_Net        |
| GS-A_4759    | IPv4-Adressen Produkttyp zum SZZP   | 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_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_3804    | Eigenschaften eines FehlerLog-Eintrags  | 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_4541    | Nutzung der Produkttypversion zur Kompatibilitätsprüfung  | 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_5040    | Änderung der Produktversion bei Produktänderungen außerhalb von Produkttypänderungen                    | 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        |
| GS-A_5134    | Performance – KOM-LE-Fachdienst – Skalierbarkeit  | gemSpec_Perf       |
| GS-A_5139-01 | Performance – KOM-LE-Fachdienst – Verfügbarkeit   | gemSpec_Perf       |
| GS-A_5143-01 | Performance – KOM-LE-Fachdienst – Nachricht senden  | gemSpec_Perf       |
| TIP1-A_7118  | Service Monitoring und Client, I_Monitoring_Update, eindeutige Zuordnung                                | gemSpec_ServiceMon |
| TIP1-A_7119  | Service Monitoring und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen                       | gemSpec_ServiceMon |
| TIP1-A_7127  | Nutzer des Service Monitorings I_Monitoring_Update, eindeutige Zuordnung des Messwertes                 | gemSpec_ServiceMon |
| TIP1-A_7129  | Nutzer des Service Monitorings I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht | gemSpec_ServiceMon |
| TIP1-A_5568  | VZD und LDAP Client, Implementierung der LDAPv3 search Operation  | gemSpec_VZD        |
| TIP1-A_5576  | Nutzer der Schnittstelle, TUC_VZD_0002 „add_Directory_Entry“  | gemSpec_VZD        |
| TIP1-A_5578  | Nutzer der Schnittstelle, TUC_VZD_0003 „read_Directory_Entry“   | gemSpec_VZD        |



| Afo-ID               | Afo-Bezeichnung   | Quelle (Referenz)       |
|----------------------|---|-------------------------|
| TIP1-A_5580          | Nutzer der Schnittstelle, TUC_VZD_0004 „modify_Directory_Entry“           | gemSpec_VZD             |
| TIP1-A_5582          | Nutzer der Schnittstelle, TUC_VZD_0005 „delete_Directory_Entry“           | gemSpec_VZD             |
| TIP1-A_5588          | FAD, I_Directory_Application_Maintenance, Nutzung LDAP v3 oder Webservice | gemSpec_VZD             |
| TIP1-A_5589          | FAD, Implementierung der LDAPv3 Schnittstelle                             | gemSpec_VZD             |
| TIP1-A_5592-03       | FAD, KOM-LE_FA_Add_Attributes   | gemSpec_VZD             |
| TIP1-A_5601-03       | FAD, KOM-LE_FA_Modify_Attributes  | gemSpec_VZD             |
| <del>GS-A_5139</del> | <del>Performance—KOM-LE-Fachdienst—Verfügbarkeit</del>                    | <del>gemSpec_Perf</del> |
| <del>GS-A_5143</del> | <del>Performance—KOM-LE-Fachdienst—Nachricht senden</del>                 | <del>gemSpec_Perf</del> |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 Sicherheitstechnische Eignung: Zertifizierung nach Technischer Richtlinie

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Prüfung gemäß TR TR-03143 „eHealth G2-COS Konsistenz-Prüfwerkzeug“ nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Prüfberichts eines für diese Prüfung zugelassenen Prüflabors.

**Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie"**

| Afo-ID | Afo-Bezeichnung                   | Quelle (Referenz) |
|--------|-----------------------------------|-------------------|
|        | Es liegen keine Anforderungen vor |                   |

### 3.2.2 CC-Evaluierung

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer Zertifizierung gemäß Common Criteria [CC] nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

**Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"**

| Afo-ID | Afo-Bezeichnung                   | Quelle (Referenz) |
|--------|-----------------------------------|-------------------|
|        | Es liegen keine Anforderungen vor |                   |

### 3.2.3 Sicherheitsgutachten

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

**Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"**

| Afo-ID               | Afo-Bezeichnung   | Quelle (Referenz)   |
|----------------------|---|---------------------|
| GS-A_4330            | Einbringung des Komponentenzertifikats  | gemRL_TSL_SP_CP     |
| GS-A_2076-01         | kDSM: Datenschutzmanagement nach BSI  | gemSpec_DS_Anbieter |
| GS-A_2158-01         | Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen                        | gemSpec_DS_Anbieter |
| GS-A_2214-01         | kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren  | 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_3078            | Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive | gemSpec_DS_Anbieter |
| GS-A_3125            | Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip                                     | gemSpec_DS_Anbieter |
| GS-A_3130            | Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip                  | gemSpec_DS_Anbieter |
| GS-A_3139            | Krypto_Schlüssel: Dienst Schlüsselableitung   | gemSpec_DS_Anbieter |
| GS-A_3141            | Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion          | gemSpec_DS_Anbieter |
| GS-A_3149            | Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip                  | 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 |
| GS-A_5626            | kDSM: Auftragsverarbeitung  | gemSpec_DS_Anbieter |
| KOM-LE-A_216<br>4    | Passwörter nicht im Klartext speichern  | gemSpec_FD_KOMLE    |
| KOM-LE-A_216<br>6    | Keine Änderung oder Löschung des Passwortes durch Dritte  | gemSpec_FD_KOMLE    |
| KOM-LE-A_218<br>5-01 | Mail Server darf nur Nachrichten aus der TI verarbeiten   | gemSpec_FD_KOMLE    |

| Afo-ID     | Afo-Bezeichnung  | Quelle (Referenz) |
|------------|--|-------------------|
| A_17124    | TLS-Verbindungen (ECC-Migration)   | gemSpec_Krypt     |
| A_17206    | XML-Signaturen (ECC-Migration)   | gemSpec_Krypt     |
| A_18464    | TLS-Verbindungen, nicht Version 1.1  | gemSpec_Krypt     |
| A_21275-01 | TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake | gemSpec_Krypt     |
| GS-A_4359  | X.509-Identitäten für die Durchführung einer TLS-Authentifizierung         | gemSpec_Krypt     |
| GS-A_4367  | Zufallszahlengenerator   | gemSpec_Krypt     |
| GS-A_4368  | Schlüsselerzeugung   | gemSpec_Krypt     |
| GS-A_4384  | 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_4388  | DNSSEC-Kontext   | gemSpec_Krypt     |
| GS-A_5035  | Nichtverwendung des SSL-Protokolls   | gemSpec_Krypt     |
| GS-A_5322  | Weitere Vorgaben für TLS-Verbindungen                                      | gemSpec_Krypt     |
| GS-A_3839  | DNSSEC, Zonen mittels DNSSEC sichern                                       | gemSpec_Net       |
| GS-A_3841  | Nameserver-Implementierungen, Einsatz von TSIG                             | gemSpec_Net       |
| GS-A_4808  | Nameserver-Implementierungen, nichtautorisierte Zonentransfers             | gemSpec_Net       |
| GS-A_4641  | Initiale Einbringung TI-Vertrauensanker                                    | gemSpec_PKI       |
| GS-A_4748  | Initiale Einbringung TSL-Datei   | gemSpec_PKI       |

### 3.2.4 Herstellererklärung sicherheitstechnische Eignung

In diesem Abschnitt sind alle Anforderungen an das Bestätigungsobjekt Fachdienst KOM-LE verzeichnet, deren Erfüllung der Hersteller bzw. der Anbieter zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung belegt.

**Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz)   |
|--------------|---|---------------------|
| GS-A_2355-01 | Meldung von erheblichen Schwachstellen und Bedrohungen                                      | gemSpec_DS_Anbieter |
| GS-A_4468-02 | kDSM: Jährlicher Datenschutzbericht der TI  | gemSpec_DS_Anbieter |
| GS-A_4473-01 | kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO                      | gemSpec_DS_Anbieter |
| GS-A_4478-01 | kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstößes | gemSpec_DS_Anbieter |
| GS-A_4479-01 | kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement             | 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 |

| Afo-ID            | Afo-Bezeichnung   | Quelle (Referenz)   |
|-------------------|---|---------------------|
| 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_5324-02      | kDSM: Teilnahme des Anbieters an Sitzungen des kDSM   | 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_5563         | Jahressicherheitsbericht  | gemSpec_DS_Anbieter |
| GS-A_5564         | kDSM: Ansprechpartner für Datenschutz   | gemSpec_DS_Anbieter |
| GS-A_5565         | kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO                                    | gemSpec_DS_Anbieter |
| GS-A_5566         | kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen              | gemSpec_DS_Anbieter |
| GS-A_5624         | Auditrechte der gematik zur Informationssicherheit  | gemSpec_DS_Anbieter |
| GS-A_5625         | kDSM: Auditrechte der gematik zum Datenschutz   | gemSpec_DS_Anbieter |
| KOM-LE-A_213<br>3 | Durchführung eines Accountings zur Abrechnung   | gemSpec_FD_KOMLE    |
| KOM-LE-A_213<br>7 | Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung                                      | gemSpec_FD_KOMLE    |
| KOM-LE-A_230<br>4 | Information an Nutzer zur bcc-Funktionalität  | gemSpec_FD_KOMLE    |
| A_17205           | Signatur der TSL: Signieren und Prüfen (ECC-Migration)  | gemSpec_Krypt       |
| A_17322           | TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)                     | gemSpec_Krypt       |
| A_17360           | XML-Signaturen (Dokumente) (ECC-Migration)  | gemSpec_Krypt       |
| GS-A_4367         | Zufallszahlengenerator  | gemSpec_Krypt       |
| GS-A_5526         | TLS-Renegotiation-Indication-Extension  | gemSpec_Krypt       |
| GS-A_5541         | TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM   | gemSpec_Krypt       |
| GS-A_5580-01      | TLS-Klient für betriebsunterstützende Dienste   | gemSpec_Krypt       |
| GS-A_5581         | "TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI)   | gemSpec_Krypt       |
| GS-A_4720         | Verwendung registrierter Werte für subjectDN  | gemSpec_PKI         |

### **3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung**

In diesem Abschnitt sind Anforderungen verzeichnet, deren Umsetzung im Zuge einer elektrischen, mechanischen und physikalischen Prüfung nachgewiesen werden muss. Der Nachweis erfolgt durch die Vorlage des Prüfberichts.

**Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung**

| Afo-ID | Afo-Bezeichnung                   | Quelle (Referenz) |
|--------|-----------------------------------|-------------------|
|        | Es liegen keine Anforderungen vor |                   |

---

## **4 Produktypspezifische Merkmale**

---

Nachfolgend werden die optionalen Ausprägungen des Produktyps beschrieben oder  
(nicht Zutreffendes streichen)

Es liegen keine optionalen Ausprägungen des Produktyps vor.

---

## 5 Anhang A – Verzeichnisse

---

### 5.1 Abkürzungen

| Kürzel | Erläuterung                 |
|--------|-----------------------------|
| Afo-ID | Anforderungs-Identifikation |
| CC     | Common Criteria             |

### 5.2 Tabellenverzeichnis

|  |    |
|--|----|
| Tabelle 1: Dokumente mit Anforderungen zu dem Bestätigungsobjekt .....   | 7  |
| Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" .....                                     | 8  |
| Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellereklärung" .....   | 14 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung " Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie" ..... | 17 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung" .....   | 17 |
| Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ..  | 18 |
| Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" .....   | 19 |
| Tabelle 8: Anforderungen zur elektrischen, mechanischen und physikalischen Eignung .   | 21 |

### 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                           |
| [gemZul_Best_KOM-LE] | gematik: Bestätigung Produkte<br>hier: Fachdienst-KOM-LE bzw. KOM-LE-Clientmodul |