

# Produkttypsteckbrief

## *Prüfvorschrift*

# Intermediär VSDM

Produkttypversion: 1.6.1-0  
Produkttypstatus: freigegeben

Version: 1.0.1  
Revision: 182516  
Stand: 04.12.2019  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_Intermediaer\_VSDM\_PTV\_1.6.1-0

## 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 auf Dokumentenebene | gemProdT_Intermediär_VSDM_PTV1.0.0   |
| 1.1.0             | Losübergreifende Synchronisation     | gemProdT_Intermediär_VSDM_PTV1.1.0   |
| 1.2.0             | P11-Änderungsliste                   | gemProdT_Intermediär_VSDM_PTV1.2.0   |
| 1.4.0             | Errata Release 1.4.6                 | gemProdT_Intermediär_VSDM_PTV1.4.0   |
| 1.5.0             | OPB1-Anpassung                       | gemProdT_Intermediär_VSDM_PTV1.5.0   |
| 1.5.1             | Änderungsliste (P13 und P14)         | gemProdT_Intermediär_VSDM_PTV1.5.1   |
| 1.5.1-1           | Anpassung auf Releasestand 1.6.3     | gemProdT_Intermediär_VSDM_PTV1.5.1-1 |
| 1.5.2-0           | Anpassung auf Releasestand 1.6.4     | gemProdT_Intermediär_VSDM_PTV1.5.2-0 |
| 1.5.3-0           | Anpassung auf Releasestand 2.1.2     | gemProdT_Intermediär_VSDM_PTV1.5.3-0 |
| 1.5.4-0           | Anpassung auf Releasestand 2.1.3     | gemProdT_Intermediär_VSDM_PTV1.5.4-0 |
| 1.6.0-0           | Anpassung auf Releasestand 3.1.0     | gemProdT_Intermediär_VSDM_PTV1.6.0-0 |
| 1.6.1-0           | Anpassung auf Releasestand 3.1.2     | gemProdT_Intermediär_VSDM_PTV1.6.1-0 |

### 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   | 02.10.2019 |      | freigegeben                            | gematik    |
| 1.0.1   | 04.12.19   | 2    | Version gemSpec_Perf angepasst         | 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 .....                        | 19        |
| 3.2.1 CC-Evaluierung .....  | 19        |
| 3.2.2 Sicherheitsgutachten .....  | 19        |
| 3.2.3 Herstellererklärung sicherheitstechnische Eignung .....                     | 21        |
| 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung ..... | 23        |
| <b>4 Produktypspezifische Merkmale .....</b>                                      | <b>24</b> |
| <b>5 Anhang A – Verzeichnisse .....</b>   | <b>25</b> |
| 5.1 Abkürzungen .....   | 25        |
| 5.2 Tabellenverzeichnis .....   | 25        |
| 5.3 Referenzierte Dokumente .....   | 25        |

---

## 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 Intermediär VSDM 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 Intermediär VSDM-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- 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_ServiceMon       | Spezifikation Service Monitoring   | 1.4.0   |
| gemSpec_PKI              | Übergreifende Spezifikation – Spezifikation PKI  | 2.7.0   |
| gemSpec_SST_VSDM         | Schnittstellenspezifikation Transport VSDM   | 2.5.0   |
| gemSpec_TSL              | Spezifikation TSL-Dienst   | 1.16.0  |
| gemSpec_Perf             | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform                              | 2.9.1   |
| gemSpec_St_Ampel         | Spezifikation Störungsampel  | 1.6.0   |
| gemRL_TSL_SP_CP          | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL             | 2.4.0   |
| gemSpec_DS_Anbieter      | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter                         | 1.1.0   |
| gemSpec_Net              | Übergreifende Spezifikation Netzwerk   | 1.16.0  |
| gemSpec_Krypt            | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.15.0  |
| gemSpec_OM               | Übergreifende Spezifikation Operations und Maintenance   | 1.12.0  |
| gemKPT_Test              | Testkonzept der TI   | 2.5.0   |
| gemSpec_Intermediar_VSDM | Spezifikation Intermediär VSDM   | 1.11.0  |

### 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_14596     | Intermediär VSDM: Fachdienst-Verbindungsprotokoll schreiben                                | gemSpec_Intermediär_VSDM |
| A_17216     | Intermediär VSDM: Fachmodul-Verbindungsprotokoll schreiben                                 | gemSpec_Intermediär_VSDM |
| VSDM-A_2348 | Intermediär VSDM: Ermitteln der URL des Fachdienstes                                       | gemSpec_Intermediär_VSDM |
| VSDM-A_2349 | Intermediär VSDM: Lokalisierungsinformation zwischenspeichern                              | gemSpec_Intermediär_VSDM |
| VSDM-A_2350 | Intermediär VSDM: konfigurierbare Parameter  | gemSpec_Intermediär_VSDM |
| VSDM-A_2351 | Intermediär VSDM: konfigurierbare Admissions für den Verbindungsaufbau zu den Fachdiensten | gemSpec_Intermediär_VSDM |
| VSDM-A_2353 | Intermediär VSDM: HTTP-Fehlermeldungen erstellen   | gemSpec_Intermediär_VSDM |
| VSDM-A_2356 | Intermediär VSDM: Performanceprotokoll mit Feldern schreiben                               | gemSpec_Intermediär_VSDM |
| VSDM-A_2357 | Intermediär VSDM: Performanceprotokoll für Performancevorgaben schreiben                   | gemSpec_Intermediär_VSDM |
| VSDM-A_2358 | Intermediär VSDM: Fehlerprotokoll mit Feldern schreiben                                    | gemSpec_Intermediär_VSDM |



|             |   |                          |
|-------------|---|--------------------------|
| VSDM-A_2359 | Intermediär VSDM: Ablaufprotokoll mit Feldern schreiben                                 | gemSpec_Intermediär_VSDM |
| VSDM-A_2547 | Intermediär VSDM: konfigurierbare Parameter für den Verbindungsaufbau zum Fachmodul     | gemSpec_Intermediär_VSDM |
| VSDM-A_2548 | Intermediär VSDM: konfigurierbare Parameter für den Verbindungsaufbau zum Fachdienste   | gemSpec_Intermediär_VSDM |
| VSDM-A_2549 | Intermediär VSDM: konfigurierbare Parameter für Cipher-Suiten                           | gemSpec_Intermediär_VSDM |
| VSDM-A_2550 | Intermediär VSDM: konfigurierbare Admissions für den Verbindungsaufbau zum Fachmodul    | gemSpec_Intermediär_VSDM |
| VSDM-A_2673 | Intermediär VSDM: Vorgangsnummer bilden   | gemSpec_Intermediär_VSDM |
| VSDM-A_2704 | Intermediär VSDM: De-/Aktivieren der Protokollierung                                    | gemSpec_Intermediär_VSDM |
| VSDM-A_2706 | Intermediär VSDM: Performancevorgaben Verbindungsversuche                               | gemSpec_Intermediär_VSDM |
| VSDM-A_2707 | Intermediär VSDM: HTTP Header-Field Via hinzufügen                                      | gemSpec_Intermediär_VSDM |
| VSDM-A_2712 | Intermediär VSDM: Verzeichnisdienst aufrufen  | gemSpec_Intermediär_VSDM |
| VSDM-A_2747 | Intermediär VSDM: keine personenbezogenen Daten im Performanceprotokoll                 | gemSpec_Intermediär_VSDM |
| VSDM-A_2761 | Intermediär VSDM: Mechanismen zur Anonymisierung  | gemSpec_Intermediär_VSDM |
| VSDM-A_2940 | Intermediär VSDM: Verbot zum Speicherung von personenbezogene Daten in Protokolldateien | gemSpec_Intermediär_VSDM |
| GS-A_4384   | TLS-Verbindungen  | gemSpec_Krypt            |
| GS-A_5131   | Hash-Algorithmus bei OCSP/CertID  | gemSpec_Krypt            |
| A_17824     | Zentrale Dienste der TI-Plattform, Nutzung von IPv6                                     | gemSpec_Net              |
| GS-A_3832   | DNS-Protokoll, Resolver-Implementierungen   | gemSpec_Net              |
| GS-A_3834   | DNS-Protokoll, Nameserver-Implementierungen   | gemSpec_Net              |
| GS-A_3839   | DNSSEC, Zonen mittels DNSSEC sichern  | gemSpec_Net              |
| GS-A_3842   | DNS, Verwendung von iterativen queries zwischen Nameservern                             | gemSpec_Net              |
| GS-A_3930   | Nameserver-Implementierungen, TTL   | 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 |
| GS-A_3933 | NTP-Server-Implementierungen, Protokoll NTPv4   | gemSpec_Net |
| 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_4809 | Nameserver-Implementierungen, Redundanz   | 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_3816 | Festlegung sicherheitsrelevanter Fehler   | gemSpec_OM  |
| GS-A_3856 | 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 Störungsmeldung                       | 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 |
| 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_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      |
| GS-A_4145 | Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen | gemSpec_Perf     |
| GS-A_4146 | Performance – Performance-Daten erfassen                          | gemSpec_Perf     |
| GS-A_4147 | Performance – Störungssampel – Performance-Daten                  | gemSpec_Perf     |
| GS-A_4148 | Performance – Störungssampel – Ereignisnachricht bei Ausfall      | gemSpec_Perf     |
| GS-A_4149 | Performance – Reporting-Daten in Performance-Report               | gemSpec_Perf     |
| GS-A_5029 | Performance – VSDM Intermediär – Bearbeitungszeit unter Last      | gemSpec_Perf     |
| GS-A_5523 | Performance – zentrale Dienste – Redundanzlösung                  | gemSpec_Perf     |
| A_17644   | Intermediär VSDM: Zustände von Fachdienst Endpunkten              | gemSpec_SST_VSDM |
| A_17645   | Intermediär VSDM: Zustand Ausfall Fachdienst Endpunkt             | gemSpec_SST_VSDM |

|             |  |                  |
|-------------|--|------------------|
| VSDM-A_2222 | Intermediär VSDM: mit TLS-Client X.509-Zertifikat authentifizieren                       | gemSpec_SST_VSDM |
| VSDM-A_2223 | Intermediär VSDM: TLS-Server X.509-Zertifikat der Fachdienste VSDM auf Gültigkeit prüfen | gemSpec_SST_VSDM |
| VSDM-A_2225 | Fachmodul VSDM, Intermediär VSDM: TLS Session Resumption mittels Session-ID nutzen       | gemSpec_SST_VSDM |
| VSDM-A_2226 | Fachanwendung VSDM: Verbindung offen halten  | gemSpec_SST_VSDM |
| VSDM-A_2227 | Intermediär VSDM: mit TLS-Server X.509-Zertifikat authentifizieren                       | gemSpec_SST_VSDM |
| VSDM-A_2228 | Intermediär VSDM: TLS-Client X.509-Zertifikat des Fachmoduls VSDM auf Gültigkeit prüfen  | gemSpec_SST_VSDM |
| VSDM-A_2231 | Intermediär VSDM: Nachrichten nicht validieren   | gemSpec_SST_VSDM |
| VSDM-A_2233 | Intermediär VSDM: Nachrichten unverändert durchreichen                                   | gemSpec_SST_VSDM |
| VSDM-A_2234 | Intermediär VSDM: Lokalisierung der Fachdienste VSDM                                     | gemSpec_SST_VSDM |
| VSDM-A_2236 | Intermediär VSDM: keine Implementierungsdetails in Fehlermeldung                         | gemSpec_SST_VSDM |
| VSDM-A_2240 | Intermediär VSDM: eingehende Nachricht zu einer Fehlermeldung speichern                  | gemSpec_SST_VSDM |
| VSDM-A_2271 | Intermediär VSDM: HTTP Header-Feld Via   | gemSpec_SST_VSDM |
| VSDM-A_2674 | Intermediär VSDM: Anfragenachricht zu einer Fehlermeldung speichern                      | gemSpec_SST_VSDM |
| VSDM-A_3002 | Verschlüsselter Transport durch Intermediär VSDM   | gemSpec_SST_VSDM |
| VSDM-A_3022 | Intermediär VSDM: Connection Pooling zu Fachdiensten                                     | gemSpec_SST_VSDM |
| VSDM-A_3023 | Intermediär VSDM: Zusätzliche Verbindungen zu Fachdiensten                               | gemSpec_SST_VSDM |
| VSDM-A_3026 | Intermediär VSDM: kein Session Resumption zu Fachdiensten VSDM                           | gemSpec_SST_VSDM |
| VSDM-A_3027 | Fachanwendung VSDM: Bedingung Rollenprüfung für HTTPS-Verbindungsaufbau                  | gemSpec_SST_VSDM |
| VSDM-A_3028 | Intermediär VSDM: Zusätzliche Verbindungen zu Fachdiensten abbauen                       | gemSpec_SST_VSDM |

|             |   |                    |
|-------------|---|--------------------|
| VSDM-A_3068 | Intermediär VSDM: Keine Konnektor identifizierende Header   | gemSpec_SST_VSDM   |
| 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_5993 | Störungssampel und Client, I_Monitoring_Update, WebService  | gemSpec_St_Ampel   |
| TIP1-A_5996 | Störungssampel und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittlung     | gemSpec_St_Ampel   |
| TIP1-A_5997 | Nutzer der Störungssampel I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung  | gemSpec_St_Ampel   |
| TIP1-A_5998 | Nutzer der Störungssampel I_Monitoring_Update, Zertifikatsprüfung   | gemSpec_St_Ampel   |
| TIP1-A_6003 | Nutzer der Störungssampel I_Monitoring_Update, eindeutige Zuordnung des Messwertes  | gemSpec_St_Ampel   |
| 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. zusagt.

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

| Afo-ID      | Afo-Bezeichnung   | Quelle (Referenz) |
|-------------|---|-------------------|
| GS-A_2162   | Kryptographisches Material in Entwicklungs- und Testumgebungen            | gemKPT_Test       |
| TIP1-A_2724 | TBI verantwortet Betrieb RU und TU  | gemKPT_Test       |
| TIP1-A_2775 | Performance in RU   | gemKPT_Test       |
| TIP1-A_4191 | Keine Echtdaten in RU und TU  | 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_6085 | Referenzobjekte eines Produkts  | gemKPT_Test       |
| TIP1-A_6088 | Unterstützung bei Fehlernachstellung                                      | gemKPT_Test       |
| TIP1-A_6093 | Ausprägung der Referenzobjekte  | gemKPT_Test       |
| TIP1-A_6517 | Eigenverantwortlicher Test: TBV   | 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_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              |
| 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              |
| VSDM-A_2747 | Intermediär VSDM: keine personenbezogenen Daten im Performanceprotokoll                  | gemSpec_Intermediär_VSDM |
| VSDM-A_2940 | Intermediär VSDM: Verbot zur Speicherung von personenbezogenen Daten in Protokolldateien | gemSpec_Intermediär_VSDM |
| VSDM-A_2942 | Intermediär VSDM: Debugprotokoll schreiben   | gemSpec_Intermediär_VSDM |
| VSDM-A_2943 | Intermediär VSDM: Sicherheitsprotokoll schreiben   | gemSpec_Intermediär_VSDM |
| VSDM-A_3006 | Intermediär VSDM: Eintrag von SRV Resource Records in der DNS Domain der Service Zone TI | gemSpec_Intermediär_VSDM |
| A_17124     | TLS-Verbindungen (ECC-Migration)   | gemSpec_Krypt            |
| A_17205     | Signatur der TLS: 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_17775     | TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)                                | gemSpec_Krypt            |
| GS-A_4388   | DNSSEC-Kontext   | gemSpec_Krypt            |
| GS-A_5527   | TLS-Renegotiation-Indication-Extension Intermediär                                       | 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_3839 | DNSSEC, Zonen mittels DNSSEC sichern                                  | gemSpec_Net |
| GS-A_3928 | Nameserver-Implementierungen, Second Level Domainnamen                | 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 |
| GS-A_4033 | Statisches Routing TI-Übergabepunkte                                  | gemSpec_Net |
| GS-A_4759 | IPv4-Adressen Produkttyp zum SZSP                                     | gemSpec_Net |
| GS-A_4805 | Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz | gemSpec_Net |
| GS-A_4810 | DNS-SD, Format von TXT Resource Records                               | gemSpec_Net |
| GS-A_4831 | Standards für IPv4  | gemSpec_Net |
| GS-A_5089 | Nameserver-Implementierungen, private Schlüssel sicher speichern      | 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_4542 | Spezifikationsgrundlage für Produkte                                  | gemSpec_OM  |

|             |   |                    |
|-------------|---|--------------------|
| GS-A_4864   | Logging-Vorgaben nach dem Übergang zum Produktivbetrieb   | 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_3055   | Performance – zentrale Dienste – Skalierbarkeit (Anbieter)  | gemSpec_Perf       |
| GS-A_4149   | Performance – Reporting-Daten in Performance-Report   | gemSpec_Perf       |
| GS-A_5030   | Performance – VSDM Intermediär – Verfügbarkeit  | gemSpec_Perf       |
| GS-A_5073   | Performance – Intermediär VSDM – Skalierbarkeit   | gemSpec_Perf       |
| VSDM-A_3021 | Intermediär VSDM: Kein Pipelining   | gemSpec_SST_VSDM   |
| 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_5994 | Störungssampel und Client, I_Monitoring_Update, eindeutige Zuordnung                                    | gemSpec_St_Ampel   |

|             |  |                  |
|-------------|--|------------------|
| TIP1-A_5995 | Störungssampel und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen                      | gemSpec_St_Ampel |
| TIP1-A_5999 | Nutzer der Störungssampel I_Monitoring_Update, maximale HTTP-Nachrichtenlänge                      | gemSpec_St_Ampel |
| TIP1-A_6002 | Nutzer der Störungssampel I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht | gemSpec_St_Ampel |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria ist nicht erforderlich.

### 3.2.2 Sicherheitsgutachten

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

**Tabelle 4: 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:<br>verpflichtende Migrationsstrategie bei<br>Schwächung kryptographischer Primitive | gemSpec_DS_Anbieter      |
| GS-A_3125    | Schlüsselinstallation und Verteilung:<br>Dokumentation gemäß Minimalitätsprinzip  | gemSpec_DS_Anbieter      |
| GS-A_3130    | Krypto_Schlüssel_Installation: Dokumentation<br>der Schlüsselinstallation gemäß<br>Minimalitätsprinzip                  | gemSpec_DS_Anbieter      |
| GS-A_3139    | Krypto_Schlüssel: Dienst Schlüsselableitung   | gemSpec_DS_Anbieter      |
| GS-A_3141    | Krypto_Schlüssel_Ableitung: Maßnahmen bei<br>Bekanntwerden von Schwächen in der<br>Schlüsselableitungsfunktion          | gemSpec_DS_Anbieter      |
| GS-A_3149    | Krypto_Schlüssel_Archivierung:<br>Dokumentation der Schlüsselarchivierung<br>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<br>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<br>Annex A   | gemSpec_DS_Anbieter      |
| GS-A_4982-01 | Umsetzung der Maßnahmen der Norm ISO/IEC<br>27002   | gemSpec_DS_Anbieter      |
| GS-A_4983-01 | Umsetzung der Maßnahmen aus dem BSI-<br>Grundschutz   | gemSpec_DS_Anbieter      |
| GS-A_4984-01 | Befolgen von herstellerepezifischen Vorgaben  | gemSpec_DS_Anbieter      |
| GS-A_5551    | Betriebsumgebung in einem Mitgliedstaat der<br>EU bzw. des EWR  | gemSpec_DS_Anbieter      |
| GS-A_5557    | Security Monitoring   | gemSpec_DS_Anbieter      |
| GS-A_5558    | Aktive Schwachstellenscans  | gemSpec_DS_Anbieter      |
| GS-A_5626    | kDSM: Auftragsverarbeitung  | gemSpec_DS_Anbieter      |
| VSDM-A_2669  | Intermediär VSDM: Zugriff nur für autorisierte<br>Personen  | gemSpec_Intermediär_VSDM |
| VSDM-A_2748  | Intermediär VSDM: Löschen von<br>pseudonymisierten Daten in Protokollen<br>innerhalb von 180 Tagen                      | gemSpec_Intermediär_VSDM |

|             |  |                  |
|-------------|--|------------------|
| A_17124     | TLS-Verbindungen (ECC-Migration)                                   | gemSpec_Krypt    |
| A_18464     | TLS-Verbindungen, nicht Version 1.1                                | 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_5131   | Hash-Algorithmus bei OCSP/CertID                                   | 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      |
| VSDM-A_2238 | Intermediär VSDM: Nachrichten grundsätzlich nicht speichern        | gemSpec_SST_VSDM |

### 3.2.3 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 belegen.

**Tabelle 5: 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 Datenschutzverstoßes       | 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 |
| 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_5017-01 | Meldung und Behandlung von Schwachstellen   | 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_5559    | Bereitstellung Ergebnisse von Schwachstellenscans   | gemSpec_DS_Anbieter |
| GS-A_5560    | Entgegennahme und Prüfung von Meldungen der gematik   | gemSpec_DS_Anbieter |
| GS-A_5561    | Bereitstellung 24/7-Kontaktpunkt  | gemSpec_DS_Anbieter |
| GS-A_5562    | Bereitstellung Produktinformationen   | gemSpec_DS_Anbieter |
| GS-A_5563    | Jahressicherheitsbericht  | gemSpec_DS_Anbieter |
| GS-A_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 Datenschutzerfordernungen 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 |
| 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_18467   | TLS-Verbindungen, Version 1.3   | gemSpec_Krypt       |
| GS-A_5527 | TLS-Renegotiation-Indication-Extension Intermediär                                    | gemSpec_Krypt       |
| GS-A_5541 | TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM                             | gemSpec_Krypt       |
| GS-A_5580 | TLS-Klient zur Störungsampel oder zum SM (Zertifikatsprüfung)                         | 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

Anforderungen an die elektrische, physikalische oder mechanische Eignung werden von der gematik nicht erhoben.

---

## 4 Produktypspezifische Merkmale

---

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 der Produkttypversion .....                              | 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 "Sicherheitsgutachten"...              | 19 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" .....             | 21 |

### 5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| [Quelle]             | Herausgeber: Titel, Version   |
|----------------------|---|
| [CC]                 | Internationaler Standard: Common Criteria for Information Technology Security Evaluation<br><a href="https://www.commoncriteriaportal.org/cc/">https://www.commoncriteriaportal.org/cc/</a> |
| [gemRL_PruefSichEig] | gematik: Richtlinie zur Prüfung der Sicherheitseignung  |