

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

VPN-Zugangsdienst

Produkttyp Version: 1.8.5-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 381672
Stand: 09.07.2021
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_VPN_ZugD_PTV_1.8.5-0

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_VPN_ZugD_PTV1.0.0 |
| 1.1.0 | Losübergreifende Synchronisation | gemProdT_VPN_ZugD_PTV1.1.0 |
| 1.2.0 | P11-Änderungsliste | gemProdT_VPN_ZugD_PTV1.2.0 |
| 1.2.1 | P12-Änderungsliste | gemProdT_VPN_ZugD_PTV1.2.1 |
| 1.4.0 | Änderungen aus Errata 1.4.3 und 1.4.6 eingefügt | gemProdT_VPN_ZugD_PTV1.4.0 |
| 1.4.1 | Errata 1.5.2 | gemProdT_VPN_ZugD_PTV1.4.1 |
| 1.5.0 | Anpassung OPB1 | gemProdT_VPN_ZugD_PTV1.5.0 |
| 1.6.0 | Änderungslisten (P13 und P14) | gemProdT_VPN_ZugD_PTV1.6.0 |
| 1.7.0-0 | Anpassung zu Releasestand 1.6.3 | gemProdT_VPN_ZugD_PTV1.7.0-0 |
| 1.7.1-0 | Anpassung zu Releasestand 1.6.4 | gemProdT_VPN_ZugD_PTV1.7.1-0 |
| 1.7.2-0 | Errata R1.6.4-1 | gemProdT_VPN_ZugD_PTV1.7.2-0 |
| 1.7.3-0 | Errata R1.6.4-2 | gemProdT_VPN_ZugD_PTV1.7.3-0 |
| 1.7.4-0 | Anpassung an Releasestand 2.1.2 | gemProdT_VPN_ZugD_PTV1.7.4-0 |
| 1.7.5-0 | Anpassung an Releasestand 2.1.3 | gemProdT_VPN_ZugD_PTV1.7.5-0 |
| 1.8.0-0 | Anpassung an Releasestand 3.1.0 | gemProdT_VPN_ZugD_PTV1.8.0-0 |

| | | |
|---------|---|------------------------------|
| 1.8.1-0 | Anpassung an Releasestand 3.1.2 | gemProdT_VPN_ZugD_PTV1.8.1-0 |
| 1.8.2-0 | Anpassung an Releasestand 3.1.3 | gemProdT_VPN_ZugD_PTV1.8.2-0 |
| 1.8.3-0 | Anpassung an Releasestand 4.0.0 | gemProdT_VPN_ZugD_PTV1.8.3-0 |
| 1.8.4-0 | Anpassung an Releasestand 4.0.1 | gemProdT_VPN_ZugD_PTV1.8.4-0 |
| 1.8.5-0 | Anpassung an Releasestand 4.0.2 und Konn_Maintenance_21.3 | gemProdT_VPN_ZugD_PTV1.8.5-0 |

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 | Datum | Kap. | Grund der Änderung, besondere Hinweise | Bearbeiter |
|----------------|--------------|-------------|---|-------------------|
| 1.0.0 | 09.07.21 | | freigegeben | gematik |

Inhaltsverzeichnis

| | |
|--|-----------|
| 1 Einführung | 5 |
| 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 |
| 2 Dokumente | 7 |
| 3 Blattanforderungen..... | 8 |
| 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 | 20 |
| 3.2.1 CC-Evaluierung | 20 |
| 3.2.2 Sicherheitsgutachten | 20 |
| 3.2.3 Herstellerklärung sicherheitstechnische Eignung | 23 |
| 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung | 24 |
| 4 Produkttypspezifische Merkmale | 25 |
| 5 Anhang A – Verzeichnisse | 26 |
| 5.1 Abkürzungen | 26 |
| 5.2 Tabellenverzeichnis | 26 |
| 5.3 Referenzierte Dokumente | 26 |

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 VPN-Zugangsdienst 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 VPN-Zugangsdienst-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. gemPTV_ATV_Festlegungen, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

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

Dokumente zu den Zulassungsverfahren für den 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_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.3.0 |
| gemSpec_Perf | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform | 2.1 23 .0 |
| gemSpec_VPN_ZugD | Spezifikation VPN-Zugangsdienst | 1.1 57 .0 |
| gemKPT_Test | Testkonzept der TI | 2. 78 .0 |
| gemRL_TSL_SP_CP | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL | 2. 69 .0 |
| gemSpec_Net | Übergreifende Spezifikation Netzwerk | 1. 49 . 20 .2 |
| gemSpec_TSL | Spezifikation TSL-Dienst | 1.1 89 .0 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.10. 92 |
| gemSpec_ServiceMon | Spezifikation Service Monitoring | 1.5.0 |
| gemSpec_OM | Übergreifende Spezifikation Operations und Maintenance | 1.14.0 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.1 89 . 91 |

Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

3 Blattanforderungen

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

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

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

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|---------------|--|--------------------------|
| GS-A_4371 | XML-Signaturen für nicht-qualifizierte Signaturen | gemSpec_Krypt |
| GS-A_4384 | TLS-Verbindungen | gemSpec_Krypt |
| GS-A_5339 | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität | gemSpec_Krypt |
| GS-A_5547 | gleiche VPN-IP-Adresse nach Reauthentication | gemSpec_Krypt |
| GS-A_5549 | Mindestgültigkeitszeiten IKE- und IPsec-SAs (VPN-Zugangsdienst) | gemSpec_Krypt |
| GS-A_3832 | DNS-Protokoll, Resolver-Implementierungen | gemSpec_Net |
| GS-A_3834 | DNS-Protokoll, Nameserver-Implementierungen | gemSpec_Net |
| GS-A_3835 | DNS-Protokoll, Unterstützung von DNS-SD | 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_3935 | NTP-Server-Implementierungen, Kiss-o'-Death | gemSpec_Net |
| GS-A_3936 | NTP-Server-Implementierungen, IBURST | gemSpec_Net |
| GS-A_3937 | NTP-Client-Implementierungen, Association Mode und Polling Intervall | gemSpec_Net |
| GS-A_3938 | NTP-Server-Implementierungen, Association Mode und Polling Intervall | gemSpec_Net |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|---|-------------------|
| GS-A_3945 | NTP-Server-Implementierungen, SNTP | gemSpec_Net |
| GS-A_4024 | Nutzung IP-Adressbereiche | gemSpec_Net |
| GS-A_4048 | DiffServ-Behandlung von Datenverkehr – Produkttypen | gemSpec_Net |
| GS-A_4070 | Netzwerksteuerungsprotokolle | gemSpec_Net |
| GS-A_4074 | NTP-Server-Implementierungen, Maximale Abweichung der Zeitinformation von Stratum-1- und -2-NTP-Servern | gemSpec_Net |
| GS-A_4765 | DSCP-Transport | gemSpec_Net |
| GS-A_4779-01 | Technische Anforderungen Sicherheitsgateways - keine Verbindungen bei Ausfall der Komponenten | 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_4832 | Path MTU Discovery und ICMP Response | gemSpec_Net |
| GS-A_4840 | DiffServ-Behandlung im VPN-Zugangsdienst | gemSpec_Net |
| GS-A_4847 | Produkttyp VPN-Zugangsdienst, DNSSEC im Namensraum Transportnetz | gemSpec_Net |
| GS-A_4879 | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern | gemSpec_Net |
| GS-A_4884 | Erlaubte ICMP-Types | 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_5025 | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM |
| GS-A_5054 | Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen | 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 |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|--|-------------------|
| 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_4652-01 | 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_15554 | Performance - VPN-Zugangsdienst - Anzahl VPN-Tunnel | gemSpec_Perf |
| A_15574 | Performance - VPN Zugangsdienst - Performance Daten (IPsec mittlerer Datendurchsatz) | gemSpec_Perf |
| A_17671 | Performance - Rohdaten-Performance-Berichte - Format des Performance-Berichts | gemSpec_Perf |
| A_17678 | Performance - Rohdaten-Performance-Berichte - Übermittlung | gemSpec_Perf |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|---|--------------------|
| 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_20155 | Performance - Erfassung von Rohdaten - VPN-Zugangsdienst | gemSpec_Perf |
| GS-A_4145 | Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen | gemSpec_Perf |
| GS-A_4146-01 | Performance – Performance-Daten erfassen | gemSpec_Perf |
| GS-A_4162 | Performance – Namensdienst – Bearbeitungszeit unter Last | gemSpec_Perf |
| GS-A_4163 | Performance – Zeitdienst – Durchsatz | gemSpec_Perf |
| GS-A_4168 | Performance – VPN-Zugangsdienst – Bearbeitungszeit | gemSpec_Perf |
| GS-A_4170 | Performance – VPN-Zugangsdienst – Durchsatz | gemSpec_Perf |
| GS-A_5331 | Performance – zentrale Dienste – TLS-Handshake | gemSpec_Perf |
| 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 |
| A_13506 | VPN-Zugangsdienst, Liveness Check VPN-Konzentrator | gemSpec_VPN_ZugD |
| A_13542 | VPN-Zugangsdienst, SIS ohne Proxy-Konfiguration | gemSpec_VPN_ZugD |
| A_14623 | VPN-Zugangsdienst, Zeichensatz der ContractID | gemSpec_VPN_ZugD |
| A_14646 | VPN-Zugangsdienst, kryptographischen Vorgaben für den Registrierungsserver | gemSpec_VPN_ZugD |
| A_17118 | VPN-Zugangsdienst und Konnektor (PTV 4 und höher), Verwendung erweiterter Sequenznummern | gemSpec_VPN_ZugD |
| A_17169 | VPN-Zugangsdienst, Fragmentierung der IKEv2-Nachrichten | gemSpec_VPN_ZugD |
| A_17171 | VPN-Zugangsdienst, IPv6-Adressierung der Nameserver Internet | gemSpec_VPN_ZugD |
| A_17173 | VPN-Zugangsdienst, IPv6 Resource Records im Nameserver Internet | gemSpec_VPN_ZugD |
| A_17180 | VPN-Zugangsdienst, IPv6-Adressierung Registrierungsserver | gemSpec_VPN_ZugD |
| A_17181 | VPN-Zugangsdienst, IPv6-Adressierung der Internetschnittstellen der VPN-Konzentratoren | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|--|-------------------|
| A_17288 | VPN-Zugangsdienst, Unterstützung der kryptographischen Vorgaben | gemSpec_VPN_ZugD |
| A_21159 | VPN-Zugangsdienst, Operation sendData | gemSpec_VPN_ZugD |
| A_21160-01 | Bereitstellung von Betriebsdaten | gemSpec_VPN_ZugD |
| A_21161 | Bereitstellung öffentlicher IP-Adressen | gemSpec_VPN_ZugD |
| TIP1-A_4282 | VPN-Zugangsdienst, Eindeutiger FQDN für VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4285 | VPN-Zugangsdienst, Umschaltzeiten am Internetzugang | gemSpec_VPN_ZugD |
| TIP1-A_4286 | VPN-Zugangsdienst, keine TI-Tunnel bei fehlender TI-Verbindung | gemSpec_VPN_ZugD |
| TIP1-A_4287 | VPN-Zugangsdienst, keine SIS-Tunnel bei fehlender SIS-Internetverbindung | gemSpec_VPN_ZugD |
| TIP1-A_4288 | VPN-Zugangsdienst, redundante Anbindung an die TI | gemSpec_VPN_ZugD |
| TIP1-A_4289 | VPN-Zugangsdienst, Service-Zone TI | gemSpec_VPN_ZugD |
| TIP1-A_4290 | VPN-Zugangsdienst, Redundanz der VPN-Konzentratoren im VPN-Konzentrator-Standort | gemSpec_VPN_ZugD |
| TIP1-A_4291 | VPN-Zugangsdienst, standortübergreifende Redundanz der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4292 | VPN-Zugangsdienst, Härtung des VPN-Konzentrators | gemSpec_VPN_ZugD |
| TIP1-A_4293 | VPN-Zugangsdienst, IPv4-Adressierung der Internetschnittstellen der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4300 | VPN-Zugangsdienst, Performance Authentisierung/Autorisierung | gemSpec_VPN_ZugD |
| TIP1-A_4302 | VPN-Zugangsdienst, Nameserver mit rekursiver Funktion im Namensraum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4303 | VPN-Zugangsdienst, Nameserver mit autoritativer Funktion im Namensraum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4305 | VPN-Zugangsdienst, IPv4-Adressierung Nameserver Internet | gemSpec_VPN_ZugD |
| TIP1-A_4306 | VPN-Zugangsdienst, Nameserver Namensraum TI | gemSpec_VPN_ZugD |
| TIP1-A_4309 | VPN-Zugangsdienst, Nameserver im Namensraum SIS | gemSpec_VPN_ZugD |
| TIP1-A_4315 | VPN-Zugangsdienst, Bildung von AAA-Zugangsdaten aus Zertifikaten | gemSpec_VPN_ZugD |
| TIP1-A_4321 | VPN-Zugangsdienst, IP-Adresse des Autorisierungsservers | gemSpec_VPN_ZugD |
| TIP1-A_4322 | VPN-Zugangsdienst, http-Forwarder - Bereitstellung | gemSpec_VPN_ZugD |
| TIP1-A_4325 | VPN-Zugangsdienst, http-Forwarder - Absenderadresse | gemSpec_VPN_ZugD |
| TIP1-A_4328 | VPN-Zugangsdienst, Anzahl der Stratum-2-NTP-Server | gemSpec_VPN_ZugD |
| TIP1-A_4330 | VPN-Zugangsdienst, Synchronisierung der Konnektoren | gemSpec_VPN_ZugD |
| TIP1-A_4334 | VPN-Zugangsdienst, Adressierung des SIS | gemSpec_VPN_ZugD |
| TIP1-A_4340-01 | VPN-Zugangsdienst, Richtlinien für den Paketfilter zum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4345 | VPN-Zugangsdienst SIS, Application Layer Gateway | gemSpec_VPN_ZugD |
| TIP1-A_4347 | VPN-Zugangsdienst SIS, Filter für aktive Inhalte | gemSpec_VPN_ZugD |
| TIP1-A_4348 | VPN-Zugangsdienst SIS, URL-Filter | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------|
| TIP1-A_4350 | VPN-Zugangsdienst und Konnektor, ESP | gemSpec_VPN_ZugD |
| TIP1-A_4351 | VPN-Zugangsdienst und Konnektor (PTV 1 bis 3), Auswertung der Sequenznummern | gemSpec_VPN_ZugD |
| TIP1-A_4352 | VPN-Zugangsdienst und Konnektor, Fenster für die Auswertung der Sequenznummern | gemSpec_VPN_ZugD |
| TIP1-A_4353 | VPN-Zugangsdienst und Konnektor, Internet Key Exchange Version 2 | gemSpec_VPN_ZugD |
| TIP1-A_4354 | VPN-Zugangsdienst und Konnektor, NAT-Traversal | gemSpec_VPN_ZugD |
| TIP1-A_4355 | VPN-Zugangsdienst und Konnektor, Dynamic Address Update | gemSpec_VPN_ZugD |
| TIP1-A_4357 | VPN-Zugangsdienst und Konnektor, Peer Liveness Detection | gemSpec_VPN_ZugD |
| TIP1-A_4364 | VPN-Zugangsdienst, DiffServ-Behandlung zwischen VPN-Konzentrator und Transportnetz Internet | gemSpec_VPN_ZugD |
| TIP1-A_4367 | VPN-Zugangsdienst, DiffServ-Behandlung zwischen VPN-Zugangsdienst und Zentralem Netz | gemSpec_VPN_ZugD |
| TIP1-A_4371 | VPN-Zugangsdienst, Identität zur Authentisierung des VPN-Konzentrators TI beim Konnektor | gemSpec_VPN_ZugD |
| TIP1-A_4372 | VPN-Zugangsdienst, Ablauf des IPsec-Verbindungsaufbaus zur TI | gemSpec_VPN_ZugD |
| TIP1-A_4389 | VPN-Zugangsdienst, I_Secure_Channel_Tunnel::disconnect | gemSpec_VPN_ZugD |
| TIP1-A_4390 | VPN-Zugangsdienst und Konnektor, Operation registerKonnektor | gemSpec_VPN_ZugD |
| TIP1-A_4391 | VPN-Zugangsdienst und Konnektor, Operation deregisterKonnektor | gemSpec_VPN_ZugD |
| TIP1-A_4392 | VPN-Zugangsdienst und Konnektor, Operation registerStatus | gemSpec_VPN_ZugD |
| TIP1-A_4395 | VPN-Zugangsdienst, Identität zur Authentisierung des VPN-Konzentrators SIS beim Konnektor | gemSpec_VPN_ZugD |
| TIP1-A_4396 | VPN-Zugangsdienst, Ablauf des IPsec-Verbindungsaufbaus Richtung Internet | gemSpec_VPN_ZugD |
| TIP1-A_4398 | VPN-Zugangsdienst, I_Secure_Internet_Tunnel::disconnect | gemSpec_VPN_ZugD |
| TIP1-A_4475 | VPN-Zugangsdienst, Performance Authentisierung/Autorisierung bei Standortausfall | gemSpec_VPN_ZugD |
| TIP1-A_4479 | VPN-Zugangsdienst, maximale Zeitabweichung der Stratum-2-NTP-Server | gemSpec_VPN_ZugD |
| TIP1-A_4481 | VPN-Zugangsdienst, Kommunikation zwischen Service-Zonen und Zugangszonen | gemSpec_VPN_ZugD |
| TIP1-A_4482 | VPN-Zugangsdienst, Kommunikation zwischen Konnektoren | gemSpec_VPN_ZugD |
| TIP1-A_4484 | Routing VPN-Zugangsdienst TI | gemSpec_VPN_ZugD |
| TIP1-A_4485 | Routing VPN-Zugangsdienst Bestandsnetze | gemSpec_VPN_ZugD |
| TIP1-A_4486 | Routing VPN-Zugangsdienst TI, lokale Dienste | gemSpec_VPN_ZugD |
| TIP1-A_4487 | Routing VPN-Zugangsdienst SIS | gemSpec_VPN_ZugD |
| TIP1-A_4490 | DiffServ-Markierung durch SIS | gemSpec_VPN_ZugD |
| TIP1-A_4491-02 | VPN-Zugangsdienst, Registrierungsserver Fehlermeldungen | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|--|-------------------|
| TIP1-A_4492 | VPN-Zugangsdienst, Zuweisung der Adressen, Verhinderung der Profilbildung | gemSpec_VPN_ZugD |
| TIP1-A_5117 | Anonymisierung | gemSpec_VPN_ZugD |
| TIP1-A_5155 | VPN-Zugangsdienst SIS, Verhinderung Verbindungsaufbau aus dem Internet | gemSpec_VPN_ZugD |
| TIP1-A_5389 | VPN-Zugangsdienst, zyklische Prüfung der C.NK.VPN und C.HCI.OSIG Zertifikate | gemSpec_VPN_ZugD |
| TIP1-A_5390 | VPN-Zugangsdienst, gesperrtes C.HCI.OSIG oder gesperrtes C.NK.VPN Zertifikat | gemSpec_VPN_ZugD |
| TIP1-A_5391 | VPN-Zugangsdienst, Unterstützung von Änderungen der Registrierung | gemSpec_VPN_ZugD |
| TIP1-A_5451 | VPN-Zugangsdienst, IPsec-Verbindungen bei Komponentenausfall beenden | gemSpec_VPN_ZugD |
| TIP1-A_5709 | VPN-Zugangsdienst, bereitgestellte Zertifikate | gemSpec_VPN_ZugD |
| TIP1-A_6748 | Traffic Selectoren VPN-Zugangsdienst TI | gemSpec_VPN_ZugD |
| TIP1-A_4491-01 | VPN-Zugangsdienst, Registrierungsserver Fehlermeldungen | gemSpec_VPN_ZugD |

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) |
|----------------|--|-------------------|
| A_20065 | Nutzung der Dokumententemplates der gematik | gemKPT_Test |
| GS-A_2162 | Kryptographisches Material in Entwicklungs- und Testumgebungen | gemKPT_Test |
| TIP1-A_2724 | TBI verantwortet Betrieb RU und TU | gemKPT_Test |
| TIP1-A_2736 | Testwerkzeug Man-in-the-Middle-Box | gemKPT_Test |
| TIP1-A_2775 | Performance in RU | gemKPT_Test |
| TIP1-A_2805 | Zeitnahe Anpassung von Produktkonfigurationen | gemKPT_Test |
| TIP1-A_4191 | Keine Echtdaten in RU und TU | gemKPT_Test |
| TIP1-A_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_6517-01 | Eigenverantwortlicher Test: TBI | gemKPT_Test |
| TIP1-A_6518 | Eigenverantwortlicher Test: TDI | gemKPT_Test |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------|
| 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 |
| TIP1-A_7333 | Parallelbetrieb von Release oder Produkttypversion | gemKPT_Test |
| TIP1-A_7334 | Risikoabschätzung bezüglich der Interoperabilität | gemKPT_Test |
| TIP1-A_7335 | Bereitstellung der Testdokumentation | gemKPT_Test |
| TIP1-A_7358 | Qualität des Produktmusters | gemKPT_Test |
| A_17124 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| A_17125 | IKE-Schlüsselaushandlung für IPsec (ECC-Migration) | gemSpec_Krypt |
| A_17126 | IPsec-Kontext -- Verschlüsselte Kommunikation (ECC-Migration) | gemSpec_Krypt |
| 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_17775 | TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration) | gemSpec_Krypt |
| GS-A_5508 | IPsec make_before_break | gemSpec_Krypt |
| GS-A_5526 | TLS-Renegotiation-Indication-Extension | 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_3930 | Nameserver-Implementierungen, TTL | gemSpec_Net |
| GS-A_3931 | DNSSEC-Protokoll, Nameserver-Implementierungen | gemSpec_Net |
| GS-A_3941 | Produkttyp VPN-Zugangsdienst, Stratum 2 | gemSpec_Net |
| GS-A_4009 | Übertragungstechnologie auf OSI-Schicht LAN | gemSpec_Net |
| GS-A_4010 | Standards für IPv6 | gemSpec_Net |
| GS-A_4011 | Unterstützung des Dual-Stack Mode | gemSpec_Net |
| GS-A_4012 | Leistungsanforderungen an den Dual-Stack Mode | gemSpec_Net |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|--|-------------------|
| GS-A_4013 | Nutzung von UDP/TCP-Portbereichen | gemSpec_Net |
| GS-A_4018 | Dokumentation UDP/TCP-Portbereiche Anbieter | gemSpec_Net |
| GS-A_4027 | Reporting IP-Adressbereiche | gemSpec_Net |
| GS-A_4033 | Statisches Routing TI-Übergabepunkte | gemSpec_Net |
| GS-A_4036 | Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen | gemSpec_Net |
| GS-A_4037 | Unterstützung der DiffServ-Architektur | gemSpec_Net |
| GS-A_4053 | Ingress und Egress Filtering | gemSpec_Net |
| GS-A_4054 | Paketfilter Default Deny | gemSpec_Net |
| GS-A_4057-01 | Technische Anforderungen Sicherheitsgateways – Betriebssoftware | gemSpec_Net |
| GS-A_4061 | Sicherheitskomponenten Zugangsdienst | gemSpec_Net |
| GS-A_4066 | Umsetzung Sicherheitsgateway-Regeln | gemSpec_Net |
| GS-A_4067 | Reporting Sicherheitsgateway-Regeln | gemSpec_Net |
| GS-A_4069 | Erlaubter Verkehr Produkttypen | gemSpec_Net |
| GS-A_4759 | IPv4-Adressen Produkttyp zum SZZP | gemSpec_Net |
| GS-A_4763 | Einsatz von Hochverfügbarkeitsprotokollen | gemSpec_Net |
| GS-A_4778-01 | Technische Anforderungen Sicherheitsgateways - Verbindungen nach Erstinstallation | 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_4820 | Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform | gemSpec_Net |
| GS-A_4831 | Standards für IPv4 | gemSpec_Net |
| GS-A_4841 | Unterstützung von Dienstklassen im VPN-Zugangsdienst | gemSpec_Net |
| GS-A_4847 | Produkttyp VPN-Zugangsdienst, DNSSEC im Namensraum Transportnetz | gemSpec_Net |
| GS-A_4879 | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern | gemSpec_Net |
| GS-A_5037 | VPN-Zugangsdienst, Prozess zur Verteilung des DNSSEC Trust Anchor im Namensraum Transportnetz | 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 |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-------------|---|--------------------|
| GS-A_4541 | Nutzung der Produkttypversion zur Kompatibilitätsprüfung | gemSpec_OM |
| GS-A_5018 | Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen | gemSpec_OM |
| GS-A_5033 | Betriebsdokumentation der zentralen Produkte der TI-Plattform und anwendungsspezifischen Diensten | gemSpec_OM |
| GS-A_5038 | Festlegungen zur Vergabe einer Produktversion | gemSpec_OM |
| GS-A_5039 | Änderung der Produktversion bei Änderungen der Produkttypversion | gemSpec_OM |
| GS-A_4640 | Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung | gemSpec_PKI |
| GS-A_3055 | Performance – zentrale Dienste – Skalierbarkeit (Anbieter) | gemSpec_Perf |
| GS-A_3058 | Performance – zentrale Dienste – lineare Skalierbarkeit | gemSpec_Perf |
| GS-A_4155 | Performance – zentrale Dienste – Verfügbarkeit | gemSpec_Perf |
| GS-A_4165 | Performance – Zeitdienst – Verfügbarkeit | gemSpec_Perf |
| GS-A_5015 | Performance – VPN-Zugangsdienst – Volumenmessung im SIS | gemSpec_Perf |
| GS-A_5028 | Performance – zentrale Dienste – Verfügbarkeit Produktivbetrieb | gemSpec_Perf |
| GS-A_5510 | Performance – VPN-Zugangsdienst – IPSec-Tunnel TI und SIS | gemSpec_Perf |
| GS-A_5523 | Performance – zentrale Dienste – Redundanzlösung | gemSpec_Perf |
| GS-A_5545 | Performance – VPN-Zugangsdienst – IPSec-Tunnel TI und SIS Konfigurationseinstellungen | 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 |
| A_21339-01 | Löschung von Betriebsdaten | gemSpec_VPN_ZugD |
| A_21611 | Information des Konnektorbetreibers auf Grund von Betriebsdaten | gemSpec_VPN_ZugD |
| A_21612 | Betriebsdaten: Zweckbindung und Weiterleitung | gemSpec_VPN_ZugD |
| TIP1-A_4277 | VPN-Zugangsdienst, Physische Trennung der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4278 | VPN-Zugangsdienst, Geografische Verteilung der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4279 | VPN-Zugangsdienst, Mindestanzahl Standorte VPN-Konzentrator | gemSpec_VPN_ZugD |
| TIP1-A_4281 | VPN-Zugangsdienst, NAT an der Schnittstelle zum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4282 | VPN-Zugangsdienst, Eindeutiger FQDN für VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4284 | VPN-Zugangsdienst, Redundanter Internetzugang | gemSpec_VPN_ZugD |
| TIP1-A_4285 | VPN-Zugangsdienst, Umschaltzeiten am Internetzugang | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-------------|--|-------------------|
| TIP1-A_4286 | VPN-Zugangsdienst, keine TI-Tunnel bei fehlender TI-Verbindung | gemSpec_VPN_ZugD |
| TIP1-A_4287 | VPN-Zugangsdienst, keine SIS-Tunnel bei fehlender SIS-Internetverbindung | gemSpec_VPN_ZugD |
| TIP1-A_4288 | VPN-Zugangsdienst, redundante Anbindung an die TI | gemSpec_VPN_ZugD |
| TIP1-A_4289 | VPN-Zugangsdienst, Service-Zone TI | gemSpec_VPN_ZugD |
| TIP1-A_4290 | VPN-Zugangsdienst, Redundanz der VPN-Konzentratoren im VPN-Konzentrator-Standort | gemSpec_VPN_ZugD |
| TIP1-A_4291 | VPN-Zugangsdienst, standortübergreifende Redundanz der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4293 | VPN-Zugangsdienst, IPv4-Adressierung der Internetschnittstellen der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4294 | VPN-Zugangsdienst, Adressen des SIS zum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4295 | VPN-Zugangsdienst, eigene Domain für VPN-Konzentrator-FQDN | gemSpec_VPN_ZugD |
| TIP1-A_4296 | VPN-Zugangsdienst, Namensauflösung durch SRV-Record | gemSpec_VPN_ZugD |
| TIP1-A_4297 | VPN-Zugangsdienst, Nutzung der SRV-Records zu betrieblichen Zwecken | gemSpec_VPN_ZugD |
| TIP1-A_4301 | VPN-Zugangsdienst, Durchsatz Verbindung zum Transportnetz Internet | gemSpec_VPN_ZugD |
| TIP1-A_4302 | VPN-Zugangsdienst, Nameserver mit rekursiver Funktion im Namensraum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4303 | VPN-Zugangsdienst, Nameserver mit autoritativer Funktion im Namensraum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4305 | VPN-Zugangsdienst, IPv4-Adressierung Nameserver Internet | gemSpec_VPN_ZugD |
| TIP1-A_4306 | VPN-Zugangsdienst, Nameserver Namensraum TI | gemSpec_VPN_ZugD |
| TIP1-A_4307 | VPN-Zugangsdienst, Bereitstellung Nameserver TI | gemSpec_VPN_ZugD |
| TIP1-A_4308 | VPN-Zugangsdienst, Adressierung des Nameservers TI | gemSpec_VPN_ZugD |
| TIP1-A_4309 | VPN-Zugangsdienst, Nameserver im Namensraum SIS | gemSpec_VPN_ZugD |
| TIP1-A_4310 | VPN-Zugangsdienst, Bereitstellung Nameserver SIS | gemSpec_VPN_ZugD |
| TIP1-A_4311 | VPN-Zugangsdienst, Adressierung Nameserver SIS | gemSpec_VPN_ZugD |
| TIP1-A_4312 | VPN-Zugangsdienst, Bereitstellung Registrierungsserver | gemSpec_VPN_ZugD |
| TIP1-A_4314 | VPN-Zugangsdienst, IPv4-Adressierung Registrierungsserver | gemSpec_VPN_ZugD |
| TIP1-A_4315 | VPN-Zugangsdienst, Bildung von AAA-Zugangsdaten aus Zertifikaten | gemSpec_VPN_ZugD |
| TIP1-A_4316 | VPN-Zugangsdienst, Autorisierung über Protokoll | gemSpec_VPN_ZugD |
| TIP1-A_4317 | VPN-Zugangsdienst, Profilzuweisung durch Autorisierungsserver | gemSpec_VPN_ZugD |
| TIP1-A_4318 | VPN-Zugangsdienst, ACL-Zuweisung | gemSpec_VPN_ZugD |
| TIP1-A_4319 | VPN-Zugangsdienst, Verteilung des Autorisierungsservers | gemSpec_VPN_ZugD |
| TIP1-A_4323 | VPN-Zugangsdienst, http-Forwarder - Verteilung | gemSpec_VPN_ZugD |
| TIP1-A_4326 | VPN-Zugangsdienst, http-Forwarder - kein Cache | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-------------|---|-------------------|
| TIP1-A_4327 | VPN-Zugangsdienst, http-Forwarder - IP-Adresse | gemSpec_VPN_ZugD |
| TIP1-A_4328 | VPN-Zugangsdienst, Anzahl der Stratum-2-NTP-Server | gemSpec_VPN_ZugD |
| TIP1-A_4331 | VPN-Zugangsdienst, Adressierung der NTP-Server | gemSpec_VPN_ZugD |
| TIP1-A_4332 | VPN-Zugangsdienst, Verteilung des SIS | gemSpec_VPN_ZugD |
| TIP1-A_4334 | VPN-Zugangsdienst, Adressierung des SIS | gemSpec_VPN_ZugD |
| TIP1-A_4335 | VPN-Zugangsdienst, Bereitstellung der öffentlichen Adressen | gemSpec_VPN_ZugD |
| TIP1-A_4337 | VPN-Zugangsdienst, Physisch getrennte Schnittstellen | gemSpec_VPN_ZugD |
| TIP1-A_4338 | VPN-Zugangsdienst, Sicherung zum Transportnetz Internet durch Paketfilter | gemSpec_VPN_ZugD |
| TIP1-A_4339 | VPN-Zugangsdienst, Platzierung Paketfilters Internet | gemSpec_VPN_ZugD |
| TIP1-A_4341 | VPN-Zugangsdienst, Erkennung von Angriffen | gemSpec_VPN_ZugD |
| TIP1-A_4344 | VPN-Zugangsdienst SIS, Maßnahmen gegen Schadsoftware | gemSpec_VPN_ZugD |
| TIP1-A_4346 | VPN-Zugangsdienst SIS, Paketfilter | gemSpec_VPN_ZugD |
| TIP1-A_4349 | VPN-Zugangsdienst und Konnektor, IPsec-Protokoll | gemSpec_VPN_ZugD |
| TIP1-A_4368 | VPN-Zugangsdienst, DiffServ-Behandlung SIS zum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4369 | VPN-Zugangsdienst, Festlegung der Schnittstellen | gemSpec_VPN_ZugD |
| TIP1-A_4370 | VPN-Zugangsdienst, Schnittstelle I_Secure_Channel_Tunnel | gemSpec_VPN_ZugD |
| TIP1-A_4387 | VPN-Zugangsdienst, Adressblöcke für VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4394 | VPN-Zugangsdienst, Schnittstelle I_Secure_Internet_Tunnel | gemSpec_VPN_ZugD |
| TIP1-A_4399 | VPN-Zugangsdienst, Prozess Änderung der Sicherheitsleistungen des SIS | gemSpec_VPN_ZugD |
| TIP1-A_4472 | VPN-Zugangsdienst, Adressierung der Service-Zone TI | gemSpec_VPN_ZugD |
| TIP1-A_4473 | VPN-Zugangsdienst, Verhalten der Konzentratoren bei Vollausslastung | gemSpec_VPN_ZugD |
| TIP1-A_4476 | VPN-Zugangsdienst, Durchsatz Verbindung zum Zentralen Netz TI | gemSpec_VPN_ZugD |
| TIP1-A_4477 | VPN-Zugangsdienst, Synchronisierung der Komponenten mit den Stratum-2-NTP-Servern | gemSpec_VPN_ZugD |
| TIP1-A_4478 | VPN-Zugangsdienst, Synchronisierung der Komponenten mit Ersatzverfahren | gemSpec_VPN_ZugD |
| TIP1-A_4480 | VPN-Zugangsdienst, | gemSpec_VPN_ZugD |
| TIP1-A_4481 | VPN-Zugangsdienst, Kommunikation zwischen Service-Zonen und Zugangszonen | gemSpec_VPN_ZugD |
| TIP1-A_4482 | VPN-Zugangsdienst, Kommunikation zwischen Konnektoren | gemSpec_VPN_ZugD |
| TIP1-A_4488 | Bandbreiten innerhalb des VPN-Zugangsdienstes | gemSpec_VPN_ZugD |
| TIP1-A_4489 | DiffServ-Behandlung im alternativen Zugangsnetz | gemSpec_VPN_ZugD |
| TIP1-A_4495 | VPN-Zugangsdienst, Nutzung der ContractID | gemSpec_VPN_ZugD |
| TIP1-A_4498 | VPN-Zugangsdienst, Prozess Abschluss, Ändern und Auflösen des Vertragsverhältnisses sowie Deregistrierung von Konnektoren | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------------------------|--|----------------------------------|
| TIP1-A_5046 | VPN-Zugangsdienst, Sichere Speicherung des Vertrauensankers der PKI | gemSpec_VPN_ZugD |
| TIP1-A_5047 | VPN-Zugangsdienst, Gültigkeitsprüfung und Speicherung der TSL-Inhalte in lokalem Trust Store | gemSpec_VPN_ZugD |
| TIP1-A_5048 | VPN-Zugangsdienst, Schlüssel sicher speichern | gemSpec_VPN_ZugD |
| TIP1-A_5103 | VPN-Zugangsdienst, Resource Records im Nameserver Internet | gemSpec_VPN_ZugD |
| TIP1-A_5104 | VPN-Zugangsdienst, Resource Records im Nameserver TI | gemSpec_VPN_ZugD |
| TIP1-A_5105 | VPN-Zugangsdienst, Konfigurationsdaten zur Übergabe bei Vertragsabschluss | gemSpec_VPN_ZugD |
| TIP1-A_5118-01 | VPN-Zugangsdienst, Schnittstelle I_Registration_Service | gemSpec_VPN_ZugD |
| TIP1-A_5156 | VPN-Zugangsdienst SIS, Erkennung von Angriffen aus dem Internet | gemSpec_VPN_ZugD |
| TIP1-A_5418 | VPN-Zugangsdienst, Standorte VPN-Konzentrator RU und TU | gemSpec_VPN_ZugD |
| TIP1-A_5710 | VPN-Zugangsdienst, Verteilung des hash&URL-Servers | gemSpec_VPN_ZugD |
| TIP1-A_5711 | VPN-Zugangsdienst, Härtung des hash&URL-Servers | gemSpec_VPN_ZugD |
| TIP1-A_5712 | VPN-Zugangsdienst, IP-Adresse des hash&URL-Servers | gemSpec_VPN_ZugD |
| TIP1-A_5713 | VPN-Zugangsdienst, Härtung des Registrierungsservers | gemSpec_VPN_ZugD |
| TIP1-A_5118 | VPN-Zugangsdienst, Schnittstelle I_Registration_Service | gemSpec_VPN_ZugD |

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria [CC] 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 |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| GS-A_2331-01 | Sicherheitsvorfalls-Management | gemSpec_DS_Anbieter |
| GS-A_2332-01 | Notfallmanagement | gemSpec_DS_Anbieter |
| GS-A_2345-01 | regelmäßige Reviews | gemSpec_DS_Anbieter |
| GS-A_3737-01 | Sicherheitskonzept | gemSpec_DS_Anbieter |
| GS-A_3753-01 | Notfallkonzept | gemSpec_DS_Anbieter |
| GS-A_3772-01 | Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen | gemSpec_DS_Anbieter |
| GS-A_4980-01 | Umsetzung der Norm ISO/IEC 27001 | gemSpec_DS_Anbieter |
| GS-A_4981-01 | Erreichen der Ziele der Norm ISO/IEC 27001 Annex A | gemSpec_DS_Anbieter |
| GS-A_4982-01 | Umsetzung der Maßnahmen der Norm ISO/IEC 27002 | gemSpec_DS_Anbieter |
| GS-A_4983-01 | Umsetzung der Maßnahmen aus dem BSI-Grundschutz | gemSpec_DS_Anbieter |
| GS-A_4984-01 | Befolgen von herstellerepezifischen Vorgaben | gemSpec_DS_Anbieter |
| GS-A_5551 | Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR | gemSpec_DS_Anbieter |
| GS-A_5557 | Security Monitoring | gemSpec_DS_Anbieter |
| GS-A_5558 | Aktive Schwachstellenscans | gemSpec_DS_Anbieter |
| GS-A_5626 | kDSM: Auftragsverarbeitung | gemSpec_DS_Anbieter |
| A_17125 | IKE-Schlüsselaushandlung für IPsec (ECC-Migration) | gemSpec_Krypt |
| A_17126 | IPsec-Kontext -- Verschlüsselte Kommunikation (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_4360 | X.509-Identitäten für die Durchführung der IPsec-Authentifizierung | gemSpec_Krypt |
| GS-A_4367 | Zufallszahlengenerator | gemSpec_Krypt |
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
| GS-A_4382 | IPsec-Kontext - Schlüsselvereinbarung | gemSpec_Krypt |
| GS-A_4383 | IPsec-Kontext – Verschlüsselte Kommunikation | 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_5339 | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität | gemSpec_Krypt |
| A_20574 | Beachtung der ISI-LANA für Übergänge zu Fremdnetzen | gemSpec_Net |
| GS-A_3839 | DNSSEC, Zonen mittels DNSSEC sichern | gemSpec_Net |
| GS-A_3841 | Nameserver-Implementierungen, Einsatz von TSIG | gemSpec_Net |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|----------------|--|-------------------|
| GS-A_4057-01 | Technische Anforderungen Sicherheitsgateways – Betriebssoftware | gemSpec_Net |
| GS-A_4062-01 | Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen | gemSpec_Net |
| GS-A_4777-01 | Technische Anforderungen Sicherheitsgateways - Dokumentation Systemfunktion | gemSpec_Net |
| GS-A_4778-01 | Technische Anforderungen Sicherheitsgateways - Verbindungen nach Erstinstallation | gemSpec_Net |
| GS-A_4808 | Nameserver-Implementierungen, nichtautorisierte Zonentransfers | 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_4847 | Produkttyp VPN-Zugangsdienst, DNSSEC im Namensraum Transportnetz | gemSpec_Net |
| GS-A_4879 | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern | gemSpec_Net |
| GS-A_5037 | VPN-Zugangsdienst, Prozess zur Verteilung des DNSSEC Trust Anchor im Namensraum Transportnetz | gemSpec_Net |
| GS-A_5089 | Nameserver-Implementierungen, private Schlüssel sicher speichern | gemSpec_Net |
| GS-A_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |
| TIP1-A_4277 | VPN-Zugangsdienst, Physische Trennung der VPN-Konzentratoren | gemSpec_VPN_ZugD |
| TIP1-A_4292 | VPN-Zugangsdienst, Härtung des VPN-Konzentrators | gemSpec_VPN_ZugD |
| TIP1-A_4337 | VPN-Zugangsdienst, Physisch getrennte Schnittstellen | gemSpec_VPN_ZugD |
| TIP1-A_4338 | VPN-Zugangsdienst, Sicherung zum Transportnetz Internet durch Paketfilter | gemSpec_VPN_ZugD |
| TIP1-A_4339 | VPN-Zugangsdienst, Platzierung Paketfilters Internet | gemSpec_VPN_ZugD |
| TIP1-A_4340-01 | VPN-Zugangsdienst, Richtlinien für den Paketfilter zum Internet | gemSpec_VPN_ZugD |
| TIP1-A_4341 | VPN-Zugangsdienst, Erkennung von Angriffen | gemSpec_VPN_ZugD |
| TIP1-A_4344 | VPN-Zugangsdienst SIS, Maßnahmen gegen Schadsoftware | gemSpec_VPN_ZugD |
| TIP1-A_4345 | VPN-Zugangsdienst SIS, Application Layer Gateway | gemSpec_VPN_ZugD |
| TIP1-A_4346 | VPN-Zugangsdienst SIS, Paketfilter | gemSpec_VPN_ZugD |
| TIP1-A_4347 | VPN-Zugangsdienst SIS, Filter für aktive Inhalte | gemSpec_VPN_ZugD |
| TIP1-A_4348 | VPN-Zugangsdienst SIS, URL-Filter | gemSpec_VPN_ZugD |
| TIP1-A_4371 | VPN-Zugangsdienst, Identität zur Authentisierung des VPN-Konzentrators TI beim Konnektor | gemSpec_VPN_ZugD |
| TIP1-A_4481 | VPN-Zugangsdienst, Kommunikation zwischen Service-Zonen und Zugangszonen | gemSpec_VPN_ZugD |
| TIP1-A_4482 | VPN-Zugangsdienst, Kommunikation zwischen Konnektoren | gemSpec_VPN_ZugD |
| TIP1-A_4495 | VPN-Zugangsdienst, Nutzung der ContractID | gemSpec_VPN_ZugD |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-------------|--|-------------------|
| TIP1-A_4497 | VPN-Zugangsdienst, sichere Speicherung des Key Signing Keys des TI Trust Anchors | gemSpec_VPN_ZugD |
| TIP1-A_5046 | VPN-Zugangsdienst, Sichere Speicherung des Vertrauensankers der PKI | gemSpec_VPN_ZugD |
| TIP1-A_5047 | VPN-Zugangsdienst, Gültigkeitsprüfung und Speicherung der TSL-Inhalte in lokalem Trust Store | gemSpec_VPN_ZugD |
| TIP1-A_5048 | VPN-Zugangsdienst, Schlüssel sicher speichern | gemSpec_VPN_ZugD |
| TIP1-A_5074 | VPN-Zugangsdienst, Einhaltung des Datenschutzes bei Protokollierung | gemSpec_VPN_ZugD |
| TIP1-A_5155 | VPN-Zugangsdienst SIS, Verhinderung Verbindungsaufbau aus dem Internet | gemSpec_VPN_ZugD |
| TIP1-A_5156 | VPN-Zugangsdienst SIS, Erkennung von Angriffen aus dem Internet | gemSpec_VPN_ZugD |

3.2.3 Herstellerklärung sicherheitstechnische Eignung

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

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| 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 |

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|--|---------------------|
| 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 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 |
| A_17124 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| 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_18467 | TLS-Verbindungen, Version 1.3 | gemSpec_Krypt |
| A_21275-01 | TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake | gemSpec_Krypt |
| GS-A_5508 | IPsec make_before_break | 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

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 "Herstellererklärung" | 14 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ... | 20 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung" | 23 |

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

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