

Produkttypsteckbrief

Prüfvorschrift

TSL-Dienst

Produkttyp Version: 2.1.0-0
Produkttyp Status: freigegeben

Version: 1.0.1
Revision: 182520
Stand: 04.12.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_TSL_PTV_2.1.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

| Produkttypversion | Beschreibung der Änderung | Referenz |
|-------------------|---|-------------------------|
| 1.0.0 | Initiale Version auf Dokumentenebene | gemProdT_TSL_PTV1.0.0 |
| 1.1.0 | Losübergreifende Synchronisation | gemProdT_TSL_PTV1.1.0 |
| 1.2.0 | P11-Änderungsliste | gemProdT_TSL_PTV1.2.0 |
| 1.3.0 | P12-Änderungsliste | gemProdT_TSL_PTV1.3.0 |
| 1.5.0 | Änderungen aus Errata 1.4.3 und 1.4.6 eingefügt | gemProdT_TSL_PTV1.5.0 |
| 1.6.0 | Anpassung OPB1 | gemProdT_TSL_PTV1.6.0 |
| 1.7.0 | Anpassung R1.6.3 | gemProdT_TSL_PTV1.7.0 |
| 1.7.0-0 | Anpassung Releasestand 1.6.3 | gemProdT_TSL_PTV1.7.0-0 |
| 1.7.0-1 | Anpassung Releasestand 1.6.4 | gemProdT_TSL_PTV1.7.0-1 |
| 1.7.0-2 | Errata 1.6.4-2 | gemProdT_TSL_PTV1.7.0-2 |
| 1.7.0-3 | Anpassung Releasestand 2.1.1 | gemProdT_TSL_PTV1.7.0-3 |
| 1.8.0-0 | Anpassung an Releasestand 2.1.2 | gemProdT_TSL_PTV1.8.0-0 |
| 1.8.1-0 | Anpassung an Releasestand 2.1.3 | gemProdT_TSL_PTV1.8.1-0 |
| 2.0.0-0 | Anpassung an Releasestand 3.1.0 | gemProdT_TSL_PTV2.0.0-0 |
| 2.0.1-0 | Anpassung an Releasestand 3.1.1 | gemProdT_TSL_PTV2.0.1-0 |
| 2.1.0-0 | Anpassung an Releasestand 3.1.2 | gemProdT_TSL_PTV2.1.0-0 |

Historie Produkttypsteckbrief

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

Produkttypversion.

| Version | Datum | Kap. | Grund der Änderung, besondere Hinweise | Bearbeiter |
|---------|------------|------|--|------------|
| 1.0.0 | 02.10.2019 | | freigegeben | gematik |
| 1.0.1 | 04.12.19 | 2 | Aktualisierung gemSpec_Perf-Version | 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..... | 17 |
| 3.2 Anforderungen zur sicherheitstechnischen Eignung | 24 |
| 3.2.1 CC-Evaluierung | 24 |
| 3.2.2 Sicherheitsgutachten | 24 |
| 3.2.3 Herstellererklärung sicherheitstechnische Eignung | 29 |
| 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung | 30 |
| 4 Produkttypspezifische Merkmale..... | 31 |
| 5 Anhang A – Verzeichnisse..... | 32 |
| 5.1 Abkürzungen | 32 |
| 5.2 Tabellenverzeichnis | 32 |
| 5.3 Referenzierte Dokumente | 32 |

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 TSL-Dienst 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 TSL-Dienst-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_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 |
| 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_OID | Spezifikation Festlegung von OIDs | 3.6.0 |

Errata

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

3 Blattanforderungen

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

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

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

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-----------|--|-------------------|
| A_17124 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| GS-A_4384 | TLS-Verbindungen | gemSpec_Krypt |
| GS-A_5131 | Hash-Algorithmus bei OCSP/CertID | gemSpec_Krypt |
| GS-A_5339 | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität | gemSpec_Krypt |
| GS-A_5340 | Signatur der TSL | 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_3842 | DNS, Verwendung von iterativen queries zwischen Nameservern | gemSpec_Net |
| GS-A_3931 | DNSSEC-Protokoll, Nameserver-Implementierungen | gemSpec_Net |
| GS-A_3932 | Abfrage der in der Topologie am nächsten stehenden Nameservers | gemSpec_Net |
| GS-A_3934 | NTP-Client-Implementierungen, Protokoll NTPv4 | gemSpec_Net |
| GS-A_3937 | NTP-Client-Implementierungen, Association Mode und Polling Intervall | gemSpec_Net |

| | | |
|-----------|---|-------------|
| GS-A_4036 | Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen | gemSpec_Net |
| GS-A_4763 | Einsatz von Hochverfügbarkeitsprotokollen | gemSpec_Net |
| GS-A_4817 | Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI | gemSpec_Net |
| GS-A_4832 | Path MTU Discovery und ICMP Response | gemSpec_Net |
| GS-A_4879 | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern | gemSpec_Net |
| GS-A_4444 | OID-Festlegung für Certificate Policies | gemSpec_OID |
| GS-A_4447 | OID-Festlegung für Feldbezeichnungen in der TSL | gemSpec_OID |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern | gemSpec_OM |
| GS-A_3702 | Inhalt der Selbstauskunft von Produkten außer Karten | 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_5025 | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM |
| A_15676 | Reihenfolge der Elemente im SubjectDN von X.509-Zertifikaten | gemSpec_PKI |
| A_17686 | TSL-Signer-CA Cross-Zertifikate (ECC-Migration) | gemSpec_PKI |
| A_17687 | TSL-Signer-CA Cross-Zertifikate – Attributsbelegung (ECC-Migration) | gemSpec_PKI |
| 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_4589 | EE-Namen für Test-PKI der TI | gemSpec_PKI |
| GS-A_4590 | Zertifikatsprofile für Test-PKI | 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_4644 | TSL-Vertrauensankerwechsel | gemSpec_PKI |
| GS-A_4645 | TSL-Signatur ab Aktivierungsdatum neuer TI-Vertrauensanker | 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_4669 | Umsetzung Statusprüfdienst | gemSpec_PKI |

| | | |
|-----------|--|-------------|
| GS-A_4674 | OCSP-Requests gemäß [RFC2560] und [Common-PKI] | gemSpec_PKI |
| GS-A_4676 | OCSP-Responses gemäß [Common-PKI] | gemSpec_PKI |
| GS-A_4677 | Spezifikationskonforme OCSP-Responses | gemSpec_PKI |
| GS-A_4678 | Signierte OCSP-Responses | gemSpec_PKI |
| GS-A_4684 | Auslassung der Signaturprüfung bei OCSP-Requests | gemSpec_PKI |
| GS-A_4686 | Statusprüfdienst – Response Status | gemSpec_PKI |
| GS-A_4687 | Statusprüfdienst – Response Status sigRequired | gemSpec_PKI |
| GS-A_4688 | Statusprüfdienst – Angabe von Zeitpunkten | gemSpec_PKI |
| GS-A_4690 | Statusprüfdienst – Status des X.509-Zertifikats | gemSpec_PKI |
| GS-A_4691 | Statusprüfdienst – X.509-Zertifikat mit Status „unknown“ | gemSpec_PKI |
| GS-A_4692 | Statusprüfdienst – Angabe Sperrzeitpunkt | gemSpec_PKI |
| GS-A_4693 | Statusprüfdienst – Positive Statement | gemSpec_PKI |
| GS-A_4694 | Betrieb von OCSP-Responder für Test-PKI-CAs | gemSpec_PKI |
| GS-A_4714 | Kodierung der Attribute in X.509-Zertifikaten | gemSpec_PKI |
| GS-A_4715 | Maximale Stringlänge der Attribute im SubjectDN | gemSpec_PKI |
| GS-A_4716 | Umgang mit überlangen Organisationsnamen im SubjectDN | gemSpec_PKI |
| GS-A_4745 | Umsetzung Zertifikatsprofil C.TSL.SIG für TSL-Dienst | gemSpec_PKI |
| GS-A_4747 | Umsetzung Zertifikatsprofil C.GEM.OCSP für TSL-Dienst | 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_4897 | Gültigkeitsdauer einer TSL | 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_5090 | Statusprüfdienst – Keine Angabe von Sperrgründen | gemSpec_PKI |

| | | |
|-------------|---|--------------------|
| GS-A_5336 | Zertifikatsprüfung nach Ablauf TSL-Graceperiod | gemSpec_PKI |
| GS-A_5517 | Schlüsselgenerationen der OCSP-Signer-Zertifikate | gemSpec_PKI |
| A_14936 | Performance - Störungsampel - Ereignisnachricht bei Ausfall zentrale Dienste | gemSpec_Perf |
| GS-A_4145 | Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen | gemSpec_Perf |
| GS-A_4146 | Performance – Performance-Daten erfassen | gemSpec_Perf |
| GS-A_4147 | Performance – Störungsampel – Performance-Daten | gemSpec_Perf |
| GS-A_4148 | Performance – Störungsampel – Ereignisnachricht bei Ausfall | gemSpec_Perf |
| GS-A_4149 | Performance – Reporting-Daten in Performance-Report | gemSpec_Perf |
| GS-A_4160 | Performance – OCSP-Responder – Performance Reporting – Daten nach Zertifikatstyp | gemSpec_Perf |
| GS-A_4854 | Performance – TSL-Dienst – Last und Parallele Downloads | gemSpec_Perf |
| GS-A_5331 | Performance – zentrale Dienste – TLS-Handshake | gemSpec_Perf |
| GS-A_5550 | Performance – OCSP Responder – Grundlast | 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_5993 | Störungsampel und Client, I_Monitoring_Update, WebService | gemSpec_St_Ampel |
| TIP1-A_5996 | Störungsampel und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittlung | gemSpec_St_Ampel |
| TIP1-A_5997 | Nutzer der Störungsampel I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung | gemSpec_St_Ampel |

| | | |
|-------------|---|------------------|
| TIP1-A_5998 | Nutzer der Störungsampel I_Monitoring_Update, Zertifikatsprüfung | gemSpec_St_Ampel |
| TIP1-A_6002 | Nutzer der Störungsampel I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht | gemSpec_St_Ampel |
| A_14492 | TSL-Datei für die Referenzumgebung (RU) | gemSpec_TSL |
| A_14493 | Schnittstelle I_TSL-Management für die RU | gemSpec_TSL |
| A_14497 | Publikation von RU-TSL und -Zertifikaten | gemSpec_TSL |
| A_14498 | I_TSL_Download: Eigene Instanz für RU-TSL in der TI | gemSpec_TSL |
| A_17658 | Separate TSL-Signer-CA für RSA und ECDSA (ECC-Migration) | gemSpec_TSL |
| A_17664 | TSL-Signer-CA-Zertifikat (RSA) als TSL-Eintrag in TSL(RSA) (ECC-Migration) | gemSpec_TSL |
| A_17665 | TSL-Signer-CA-Zertifikat (ECDSA) als TSL-Eintrag in TSL(ECC-RSA) (ECC-Migration) | gemSpec_TSL |
| A_17680 | I_TSL_Download::download_TSL: GET-Befehl (ECC-Migration) | gemSpec_TSL |
| A_17681 | I_TSL_Download::get_Hash (ECC-Migration) | gemSpec_TSL |
| A_17682 | I_TSL_Download::get_Hash: URI (ECC-Migration) | gemSpec_TSL |
| A_17683 | Verwendung von ausschließlich RSA-Elementen in TSL(RSA) (ECC-Migration) | gemSpec_TSL |
| A_17684 | Verwendung von ECC- und RSA-Elementen in TSL(ECC-RSA) (ECC-Migration) | gemSpec_TSL |
| A_17685 | Unterschiedliche Nummernkreise für die TSLSequenceNumber in der TSL(RSA) und der TSL(ECC-RSA) (ECC-Migration) | gemSpec_TSL |
| A_17931 | TSL Unspecified ServiceTypeIdIdentifier | gemSpec_TSL |
| A_17932 | TSL Unspecified ServiceName | gemSpec_TSL |
| A_17933 | TSL Unspecified DigitalId | gemSpec_TSL |
| A_17934 | TSL Unspecified ServiceStatus | gemSpec_TSL |
| A_17935 | TSL Unspecified StatusStartingTime | gemSpec_TSL |
| A_17936 | TSL Unspecified Extension | gemSpec_TSL |
| TIP1-A_3994 | Schlüsselverwaltung: zwingend unterschiedliche Schlüssel für unterschiedliche Entitäten | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_4016 | Maximale Gültigkeitsdauer des TSL-Signer-Zertifikats | gemSpec_TSL |
| TIP1-A_4027 | Bereitstellung Schnittstelle I_TSL-Management | gemSpec_TSL |
| TIP1-A_4030 | Bereitstellung I_TSL-Management:Client | gemSpec_TSL |
| TIP1-A_4031 | I_TSL-Management:Client, TSL-Eintragsanträge | gemSpec_TSL |
| TIP1-A_4032 | I_TSL-Management:Client, XML-Format | gemSpec_TSL |
| TIP1-A_4035 | TSL-Signer-CA-Zertifikat als TSL-Eintrag | gemSpec_TSL |
| TIP1-A_4038 | Standardaktualisierung: periodisch | gemSpec_TSL |
| TIP1-A_4056 | I_TSL_Download: HTTP und HTTPS für TI | gemSpec_TSL |
| TIP1-A_4057 | I_TSL_Download: HTTPS für Internet | gemSpec_TSL |
| TIP1-A_4058 | X.509-Zertifikat für HTTPS für Internet | gemSpec_TSL |
| TIP1-A_4059 | EV-SSL-Zertifikat für HTTPS für Internet | gemSpec_TSL |
| TIP1-A_4060 | TSL-Dienst: URIs | gemSpec_TSL |
| TIP1-A_4062 | I_TSL_Download::download_TSL: GET-Befehl | gemSpec_TSL |
| TIP1-A_4063 | I_TSL_Download::download_TSL: Header | gemSpec_TSL |
| TIP1-A_4064 | I_TSL_Download::download_TSL: Content-Type | gemSpec_TSL |
| TIP1-A_4065 | I_TSL_Download::download_TSL: Body | gemSpec_TSL |
| TIP1-A_4067 | I_Cert_Download: HTTPS | gemSpec_TSL |
| TIP1-A_4068 | X.509-Zertifikat für HTTPS-Verbindung I_Cert_Download | gemSpec_TSL |
| TIP1-A_4069 | EV-SSL-Zertifikat für HTTPS-Schnittstelle I_Cert_Download | gemSpec_TSL |
| TIP1-A_4070 | feste URIs I_Cert_Download | gemSpec_TSL |
| TIP1-A_4072 | I_Cert_Download::download_Cert: GET-Befehl | gemSpec_TSL |
| TIP1-A_4073 | I_Cert_Download::download_Cert: Body | gemSpec_TSL |
| TIP1-A_4074 | TSL-Signer-CA-, TSL-Signer-, Komponenten-CA- Zertifikat: Angaben | gemSpec_TSL |
| TIP1-A_4076 | Erreichbarkeit OCSP-Responder | gemSpec_TSL |
| TIP1-A_4081 | ETSI_TS_102_231 | gemSpec_TSL |
| TIP1-A_4082 | ETSI_TS_102_231 Annex B und XML-Schema | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_4083 | XML-Signatur | gemSpec_TSL |
| TIP1-A_4084 | X.509-Zertifikate, Element X509Certificate | gemSpec_TSL |
| TIP1-A_4085 | ETSI_TS_102_231 Annex B: nur erforderliche Elemente | gemSpec_TSL |
| TIP1-A_4086 | TSL ID | gemSpec_TSL |
| TIP1-A_4087 | TSL Datumsformat | gemSpec_TSL |
| TIP1-A_4088 | TSLType | gemSpec_TSL |
| TIP1-A_4089 | TSL SchemeOperatorName | gemSpec_TSL |
| TIP1-A_4090 | TSL SchemeName | gemSpec_TSL |
| TIP1-A_4091 | TSL SchemeInformationURI | gemSpec_TSL |
| TIP1-A_4092 | TSL StatusDeterminationApproach | gemSpec_TSL |
| TIP1-A_4093 | TSL Postalische Adresse | gemSpec_TSL |
| TIP1-A_4094 | TSL Policy-Angaben | gemSpec_TSL |
| TIP1-A_4095 | TSL HistoricalInformationPeriod | gemSpec_TSL |
| TIP1-A_4096 | TSL Lokalisierungspunkte | gemSpec_TSL |
| TIP1-A_4097 | TSL TSPTTradeName | gemSpec_TSL |
| TIP1-A_4098 | TSL TSPTTradeName identisch mit TSPName | gemSpec_TSL |
| TIP1-A_4099 | TSL ServiceTypeldentifier | gemSpec_TSL |
| TIP1-A_4100 | TSL ServiceName: ein Name-Element | gemSpec_TSL |
| TIP1-A_4102 | TSL ServiceName aus Subject-Feld | gemSpec_TSL |
| TIP1-A_4103 | TSL DigitalId | gemSpec_TSL |
| TIP1-A_4104 | TSL DigitalId: X.509-Zertifikat / Other-Element | gemSpec_TSL |
| TIP1-A_4105 | TSL ServiceStatus | gemSpec_TSL |
| TIP1-A_4106 | TSL ServiceSupplyPoints | gemSpec_TSL |
| TIP1-A_4107 | TSL ServiceInformationExtensions | gemSpec_TSL |
| TIP1-A_4108 | TSL ServiceInformationExtensions: Extension | gemSpec_TSL |
| TIP1-A_4110 | TSL Extension: ExtensionOID & ExtensionValue | gemSpec_TSL |
| TIP1-A_4111 | TSL Test SchemeOperatorName | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_4112 | TSL Test SchemeName | gemSpec_TSL |
| TIP1-A_4113 | TSL Test Policy-Angaben | gemSpec_TSL |
| TIP1-A_4114 | TSL Test Lokalisierungspunkte | gemSpec_TSL |
| TIP1-A_4438 | TSL-Datei für Testzwecke (TU) | gemSpec_TSL |
| TIP1-A_4443 | TSL-Zertifikate für Test- und Referenzzwecke | gemSpec_TSL |
| TIP1-A_4444 | Namen für TSL-Zertifikate für Test- und Referenzzwecke in der TU und RU | gemSpec_TSL |
| TIP1-A_4445 | Profile TSL-Zertifikate für Test- und Referenzzwecke in der TU und RU | gemSpec_TSL |
| TIP1-A_4447 | Publikation von TU-TSL und -Zertifikaten | gemSpec_TSL |
| TIP1-A_4449 | OCSP-Responder für Test-TSL-Signerzertifikat | gemSpec_TSL |
| TIP1-A_5119 | TSL-Dienst: HTTP-Komprimierung unterstützen | gemSpec_TSL |
| TIP1-A_5121 | TI-spezifische Vorgaben an die Syntax der TSL-Datei | gemSpec_TSL |
| TIP1-A_5122 | TSL DNSSEC Trust Anchor ServiceTypenIdentifier | gemSpec_TSL |
| TIP1-A_5123 | TSL DNSSEC Trust Anchor Name | gemSpec_TSL |
| TIP1-A_5124 | TSL DNSSEC Trust Anchor DigitalId | gemSpec_TSL |
| TIP1-A_5125 | TSL DNSSEC Trust Anchor ServiceStatus | gemSpec_TSL |
| TIP1-A_5126 | TSL DNSSEC Trust Anchor StatusStartingTime | gemSpec_TSL |
| TIP1-A_5128 | TSL DNSSEC Trust Anchor Extension | gemSpec_TSL |
| TIP1-A_5963 | TSL CV-Zertifikate der CVC-Root-CAs ServiceTypenIdentifier | gemSpec_TSL |
| TIP1-A_5964 | TSL CV-Zertifikate der CVC-Root-CAs Name | gemSpec_TSL |
| TIP1-A_5965 | TSL CV-Zertifikate der CVC-Root-CAs DigitalId | gemSpec_TSL |
| TIP1-A_5966 | TSL CV-Zertifikate der CVC-Root-CAs ServiceStatus | gemSpec_TSL |
| TIP1-A_5967 | TSL CV-Zertifikate der CVC-Root-CA Extension | gemSpec_TSL |
| TIP1-A_6750 | I_BNetzA_VL_Download: GET-Befehl | gemSpec_TSL |
| TIP1-A_6751 | I_BNetzA_VL_Download: Header | gemSpec_TSL |
| TIP1-A_6752 | I_BNetzA_VL_Download::download_VL: Content-Type | gemSpec_TSL |
| TIP1-A_6753 | I_BNetzA_VL_Download::download_VL: Body | gemSpec_TSL |

| | | |
|-------------|--|-------------|
| TIP1-A_6754 | I_BNetZA_VL_Download::get_Hash | gemSpec_TSL |
| TIP1-A_6755 | I_BNetZA_VL_Download::get_Hash: URI | gemSpec_TSL |
| TIP1-A_6756 | BNetZA-VL-Signer-Zertifikate in TSL aufnehmen und entfernen | gemSpec_TSL |
| TIP1-A_6760 | Pseudo-BNetZA-VL für TU und RU bereitstellen | gemSpec_TSL |
| TIP1-A_6761 | BNetZA-VL Element TrustServiceProvider | gemSpec_TSL |
| TIP1-A_6762 | BNetZA-VL Element TSPService | gemSpec_TSL |
| TIP1-A_6763 | BNetZA-VL ServiceTypeIdentifier | gemSpec_TSL |
| TIP1-A_6764 | BNetZA-VL Service Name | gemSpec_TSL |
| TIP1-A_6765 | BNetZA-VL ServiceDigitalIdentity, DigitalId und X509Certificate | gemSpec_TSL |
| TIP1-A_6766 | BNetZA-VL ServiceSupplyPoints | gemSpec_TSL |
| TIP1-A_6767 | BNetZA-VL ServiceInformationExtensions | gemSpec_TSL |
| TIP1-A_6768 | I_BNetZA_VL_Download: HTTPS für TI | gemSpec_TSL |
| TIP1-A_7219 | BNetZA-VL AdditionalServiceInformation für Umleitung von OCSP-Responder-Adressen in der TI | 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_2775 | Performance in RU | gemKPT_Test |
| TIP1-A_2805 | Zeitnahe Anpassung von Produktkonfigurationen | gemKPT_Test |
| TIP1-A_4191 | Keine Echtzeiten in RU und TU | gemKPT_Test |
| TIP1-A_5052 | Dauerhafte Verfügbarkeit in der RU | gemKPT_Test |
| TIP1-A_6079 | Updates von Referenzobjekten | gemKPT_Test |

| | | |
|-------------|---|---------------|
| TIP1-A_6080 | Softwarestand von Referenzobjekten | gemKPT_Test |
| TIP1-A_6081 | Bereitstellung der Referenzobjekte | gemKPT_Test |
| TIP1-A_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_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_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_5526 | TLS-Renegotiation-Indication-Extension | gemSpec_Krypt |

| | | |
|-----------|--|---------------|
| GS-A_5542 | TLS-Verbindungen (fatal Alert bei Abbrüchen) | gemSpec_Krypt |
| GS-A_3824 | FQDN von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform | gemSpec_Net |
| GS-A_3931 | DNSSEC-Protokoll, Nameserver-Implementierungen | gemSpec_Net |
| GS-A_4009 | Übertragungstechnologie auf OSI-Schicht LAN | gemSpec_Net |
| GS-A_4010 | Standards für IPv6 | gemSpec_Net |
| GS-A_4011 | Unterstützung des Dual-Stack Mode | gemSpec_Net |
| GS-A_4012 | Leistungsanforderungen an den Dual-Stack Mode | gemSpec_Net |
| GS-A_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_4054 | Paketfilter Default Deny | 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_4817 | Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI | 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_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_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 |
| A_17686 | TSL-Signer-CA Cross-Zertifikate (ECC-Migration) | gemSpec_PKI |
| GS-A_4257 | Hauptsitz und Betriebsstätte | gemSpec_PKI |
| GS-A_4588 | CA-Namen für Test-PKI der TI | gemSpec_PKI |
| GS-A_4640 | Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung | gemSpec_PKI |
| GS-A_4670 | Statusprüfdienst über Gültigkeitszeitraum des X.509-Zertifikats | gemSpec_PKI |
| GS-A_4679 | Signatur zu Statusauskünften von nonQES-Zertifikaten | gemSpec_PKI |
| GS-A_4685 | Statusprüfdienst - Steigerung der Performance | gemSpec_PKI |
| GS-A_4689 | Statusprüfdienst – Zeitquelle von producedAt | gemSpec_PKI |
| GS-A_4703 | CA-Zertifikatsprofil für nonQES-Zertifikate | gemSpec_PKI |
| GS-A_4704 | Nutzung von CA mit spezifischem Verwendungszweck | gemSpec_PKI |
| GS-A_4727 | PKI-Separierung von Test- und Produktivumgebung in der TI | gemSpec_PKI |
| GS-A_4738 | Eindeutige Identifizierung der OCSP-Signer-Zertifikate | gemSpec_PKI |
| GS-A_4739 | Attribute der OCSP-Signer-Zertifikate | gemSpec_PKI |
| GS-A_4742 | Eindeutige Identifizierung der TSL-Signer-Zertifikate | gemSpec_PKI |
| GS-A_4743 | Attribute der TSL-Signer-Zertifikate | gemSpec_PKI |
| GS-A_4744 | Zentrale TSL-Signer-CA-Zertifikate | gemSpec_PKI |
| GS-A_4918 | Ableitung des OCSP-Signer-Zertifikates für TSL-Dienst | gemSpec_PKI |

| | | |
|-------------|---|--------------------|
| GS-A_5214 | TSL Neuausstellung | gemSpec_PKI |
| GS-A_5514 | Verwendung separater OCSP-Signer-Zertifikate | gemSpec_PKI |
| GS-A_3055 | Performance – zentrale Dienste – Skalierbarkeit (Anbieter) | gemSpec_Perf |
| GS-A_3058 | Performance – zentrale Dienste – lineare Skalierbarkeit | gemSpec_Perf |
| GS-A_4149 | Performance – Reporting-Daten in Performance-Report | gemSpec_Perf |
| GS-A_4158 | Performance – TSL-Dienst – Verfügbarkeit | gemSpec_Perf |
| GS-A_4159 | Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast | gemSpec_Perf |
| TIP1-A_7118 | Service Monitoring und Client, I_Monitoring_Update, eindeutige Zuordnung | gemSpec_ServiceMon |
| TIP1-A_7119 | Service Monitoring und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen | gemSpec_ServiceMon |
| TIP1-A_7127 | Nutzer des Service Monitorings I_Monitoring_Update, eindeutige Zuordnung des Messwertes | gemSpec_ServiceMon |
| TIP1-A_7129 | Nutzer des Service Monitorings I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht | gemSpec_ServiceMon |
| TIP1-A_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_6003 | Nutzer der Störungssampel I_Monitoring_Update, eindeutige Zuordnung des Messwertes | gemSpec_St_Ampel |
| TIP1-A_3949 | Veröffentlichungspflicht und kritische Informationen | gemSpec_TSL |
| TIP1-A_3950 | Mitteilungspflicht bei Änderungen | gemSpec_TSL |
| TIP1-A_3951 | Vorlage der technischen Dokumentation und des Betriebskonzepts bei der gematik | gemSpec_TSL |
| TIP1-A_3953 | Anzeige von Änderung an der Gesellschafterstruktur des Betreibers | gemSpec_TSL |
| TIP1-A_3954 | Obligatorische Vorgaben für das Rollenkonzept | gemSpec_TSL |
| TIP1-A_3955 | Revisionssicherheit der Protokollierung | gemSpec_TSL |
| TIP1-A_3956 | Bereitstellung der Protokollierungsdaten | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_3958 | Verwendung des HSM gemäß Vier-Augen-Prinzip | gemSpec_TSL |
| TIP1-A_3959 | Backup-Konzept | gemSpec_TSL |
| TIP1-A_3960 | Besetzung von Rollen und Informationspflichten | gemSpec_TSL |
| TIP1-A_3961 | Durchgängige Verfügbarkeit spezifischer Rollen | gemSpec_TSL |
| TIP1-A_3962 | Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips | gemSpec_TSL |
| TIP1-A_3964 | Zugang zu Systemen für die TSL-Erzeugung | gemSpec_TSL |
| TIP1-A_3970 | Gewährleistung des Zugangs zur Betriebsstätte | gemSpec_TSL |
| TIP1-A_3972 | Rollenunterscheidung im organisatorischen Konzept | gemSpec_TSL |
| TIP1-A_3973 | Mitteilungspflicht für Zuordnung der Rollen | gemSpec_TSL |
| TIP1-A_3974 | Obligatorisches 4-Augen-Prinzip für sicherheitsrelevante Tätigkeiten | gemSpec_TSL |
| TIP1-A_3975 | Ausschluss von Rollenzuordnungen | gemSpec_TSL |
| TIP1-A_3977 | Einsicht in Dokumente für Mitarbeiter | gemSpec_TSL |
| TIP1-A_3982 | Aufbewahrungsfrist für Protokolldaten | gemSpec_TSL |
| TIP1-A_3984 | Archivierung: Relevante Daten | gemSpec_TSL |
| TIP1-A_3989 | Anzeigepflicht bei Beendigung der Dienstleistungen | gemSpec_TSL |
| TIP1-A_3991 | Fristen bei Einstellung des Betriebs | gemSpec_TSL |
| TIP1-A_3992 | Erforderliche Form bei Einstellung des Betriebs | gemSpec_TSL |
| TIP1-A_3994 | Schlüsselverwaltung: zwingend unterschiedliche Schlüssel für unterschiedliche Entitäten | gemSpec_TSL |
| TIP1-A_4011 | PKCS#11 | gemSpec_TSL |
| TIP1-A_4028 | I_TSL-Management, Bestätigung | gemSpec_TSL |
| TIP1-A_4036 | Syntaktische und semantische Prüfung der TSL | gemSpec_TSL |
| TIP1-A_4037 | Aktualisierungen: Standard und adhoc | gemSpec_TSL |
| TIP1-A_4039 | Standardaktualisierung: Berücksichtigung TSL-Eintragsanträge | gemSpec_TSL |
| TIP1-A_4042 | Prüfung von TSL-Eintragsanträgen | gemSpec_TSL |
| TIP1-A_4043 | Prüfung von Änderungsanträgen | gemSpec_TSL |
| TIP1-A_4044 | Prüfung auf ungültige Einträge | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_4045 | Übermittlung zur Freigabe | gemSpec_TSL |
| TIP1-A_4046 | Freigabe vor Veröffentlichung | gemSpec_TSL |
| TIP1-A_4049 | Prozess für Schlüsselpaargenerierung und Zertifizierung | gemSpec_TSL |
| TIP1-A_4050 | Zertifikatswechsel | gemSpec_TSL |
| TIP1-A_4051 | Auftrag für Schlüsselerzeugung TSL-Signer-CA und OCSP-Responder | gemSpec_TSL |
| TIP1-A_4052 | Auftrag für Schlüsselerzeugung, 2 Mitarbeiter | gemSpec_TSL |
| TIP1-A_4053 | Auftrag für Erzeugung, Inhalt | gemSpec_TSL |
| TIP1-A_4054 | TI-Vertrauensankerwechsel, Prozess | gemSpec_TSL |
| TIP1-A_4055 | Web-Server | gemSpec_TSL |
| TIP1-A_4066 | Web-Server I_Cert_Download | gemSpec_TSL |
| TIP1-A_4070 | feste URIs I_Cert_Download | gemSpec_TSL |
| TIP1-A_4074 | TSL-Signer-CA-, TSL-Signer-, Komponenten-CA-Zertifikat: Angaben | gemSpec_TSL |
| TIP1-A_4075 | Fingerprint TSL-Signer-CA-Zertifikat per Post | gemSpec_TSL |
| TIP1-A_4077 | Organisatorische Trennung für OCSP | gemSpec_TSL |
| TIP1-A_4078 | Sperrantrag | gemSpec_TSL |
| TIP1-A_4079 | Verfahren für Sperrung TSL-Signer-Zertifikat | gemSpec_TSL |
| TIP1-A_4109 | TSL Extension: Attribut „Critical“ | gemSpec_TSL |
| TIP1-A_4435 | I_TSL-Management, Zeitstempel | gemSpec_TSL |
| TIP1-A_4439 | Schnittstelle I_TSL-Management für Test (TU) | gemSpec_TSL |
| TIP1-A_4440 | Konzept Prozess für Schlüsselpaargenerierung und Zertifizierung | gemSpec_TSL |
| TIP1-A_4441 | Konzept Zertifikatswechsel | gemSpec_TSL |
| TIP1-A_4442 | Auftrag für Schlüsselerzeugung TSL-Signer | gemSpec_TSL |
| TIP1-A_4448 | I_TSL_Download: Eigene Instanz für TU-TSL in der TI | gemSpec_TSL |
| TIP1-A_4852 | TI-Vertrauensankerwechsel, Konzept | gemSpec_TSL |
| TIP1-A_5782 | Schlüsselbackup bei der gematik | gemSpec_TSL |

| | | |
|-------------|--|-------------|
| TIP1-A_5990 | Bezug und Nutzung bereitgestellter CVC-Root- und Cross-CV-Zertifikate sowie Prüfung des Fingerprints zum öffentlichen CVC-Root-Schlüssel | gemSpec_TSL |
| TIP1-A_6759 | Bezug einer Pseudo-BNetzA-VL für TU und RU | gemSpec_TSL |

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_2158-01 | Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen | gemSpec_DS_Anbieter |
| GS-A_2328-01 | Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes | gemSpec_DS_Anbieter |
| GS-A_2329-01 | Umsetzung der Sicherheitskonzepte | gemSpec_DS_Anbieter |
| GS-A_2331-01 | Sicherheitsvorfalls-Management | gemSpec_DS_Anbieter |
| GS-A_2332-01 | Notfallmanagement | gemSpec_DS_Anbieter |
| GS-A_2345-01 | regelmäßige Reviews | gemSpec_DS_Anbieter |
| GS-A_3078 | Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive | gemSpec_DS_Anbieter |
| GS-A_3125 | Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip | gemSpec_DS_Anbieter |
| GS-A_3130 | Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip | gemSpec_DS_Anbieter |
| GS-A_3139 | Krypto_Schlüssel: Dienst Schlüsselableitung | gemSpec_DS_Anbieter |
| GS-A_3141 | Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion | gemSpec_DS_Anbieter |

| | | |
|--------------|---|---------------------|
| GS-A_3149 | Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip | gemSpec_DS_Anbieter |
| GS-A_3737-01 | Sicherheitskonzept | gemSpec_DS_Anbieter |
| GS-A_3753-01 | Notfallkonzept | gemSpec_DS_Anbieter |
| GS-A_3772-01 | Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen | gemSpec_DS_Anbieter |
| GS-A_4980-01 | Umsetzung der Norm ISO/IEC 27001 | gemSpec_DS_Anbieter |
| GS-A_4981-01 | Erreichen der Ziele der Norm ISO/IEC 27001 Annex A | gemSpec_DS_Anbieter |
| GS-A_4982-01 | Umsetzung der Maßnahmen der Norm ISO/IEC 27002 | gemSpec_DS_Anbieter |
| GS-A_4983-01 | Umsetzung der Maßnahmen aus dem BSI-Grundschutz | gemSpec_DS_Anbieter |
| GS-A_4984-01 | Befolgen von herstellerepezifischen Vorgaben | gemSpec_DS_Anbieter |
| GS-A_5551 | Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR | gemSpec_DS_Anbieter |
| GS-A_5557 | Security Monitoring | gemSpec_DS_Anbieter |
| GS-A_5558 | Aktive Schwachstellenscans | gemSpec_DS_Anbieter |
| A_17124 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| A_18464 | TLS-Verbindungen, nicht Version 1.1 | gemSpec_Krypt |
| GS-A_4357 | X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen | gemSpec_Krypt |
| GS-A_4359 | X.509-Identitäten für die Durchführung einer TLS-Authentifizierung | gemSpec_Krypt |
| GS-A_4361 | X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen | gemSpec_Krypt |
| GS-A_4367 | Zufallszahlengenerator | gemSpec_Krypt |
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
| GS-A_4370 | Kryptographische Algorithmen für XML-Dokumente | gemSpec_Krypt |
| GS-A_4371 | XML-Signaturen für nicht-qualifizierte Signaturen | 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_4393 | Algorithmus bei der Erstellung von Hashwerten von Zertifikaten oder öffentlichen Schlüsseln | gemSpec_Krypt |
| GS-A_5035 | Nichtverwendung des SSL-Protokolls | gemSpec_Krypt |
| GS-A_5079 | Migration von Algorithmen und Schlüssellängen bei PKI-Betreibern | gemSpec_Krypt |
| GS-A_5131 | Hash-Algorithmus bei OCSP/CertID | gemSpec_Krypt |
| GS-A_5322 | Weitere Vorgaben für TLS-Verbindungen | gemSpec_Krypt |
| GS-A_5339 | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität | gemSpec_Krypt |
| GS-A_5340 | Signatur der TSL | gemSpec_Krypt |
| GS-A_4054 | Paketfilter Default Deny | gemSpec_Net |
| GS-A_4062 | Sicherheitskomponenten bei Netzübergängen zu Fremdnetzen | gemSpec_Net |
| GS-A_4879 | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern | gemSpec_Net |
| GS-A_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |
| TIP1-A_3954 | Obligatorische Vorgaben für das Rollenkonzept | gemSpec_TSL |
| TIP1-A_3955 | Revisionssicherheit der Protokollierung | gemSpec_TSL |
| TIP1-A_3957 | Standort für Backup-HSM | gemSpec_TSL |
| TIP1-A_3958 | Verwendung des HSM gemäß Vier-Augen-Prinzip | gemSpec_TSL |
| TIP1-A_3959 | Backup-Konzept | gemSpec_TSL |
| TIP1-A_3960 | Besetzung von Rollen und Informationspflichten | gemSpec_TSL |
| TIP1-A_3962 | Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips | gemSpec_TSL |
| TIP1-A_3963 | Nutzung des HSM im kontrollierten Bereich | gemSpec_TSL |
| TIP1-A_3967 | Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung | gemSpec_TSL |
| TIP1-A_3968 | Manipulationsschutz veröffentlichter Daten | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_3969 | Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems | gemSpec_TSL |
| TIP1-A_3971 | Organisatorische Trennung von anderen Rollen in TI | gemSpec_TSL |
| TIP1-A_3972 | Rollenunterscheidung im organisatorischen Konzept | gemSpec_TSL |
| TIP1-A_3974 | Obligatorisches 4-Augen-Prinzip für sicherheitsrelevante Tätigkeiten | gemSpec_TSL |
| TIP1-A_3975 | Ausschluss von Rollenzuordnungen | gemSpec_TSL |
| TIP1-A_3976 | Anforderungen an den Einsatz freier Mitarbeiter | gemSpec_TSL |
| TIP1-A_3977 | Einsicht in Dokumente für Mitarbeiter | gemSpec_TSL |
| TIP1-A_3978 | Aufzeichnung von technischen Ereignissen | gemSpec_TSL |
| TIP1-A_3979 | Aufzeichnung von organisatorischen Ereignissen | gemSpec_TSL |
| TIP1-A_3980 | Protokollierung wichtiger TSL-spezifischer Ereignisse | gemSpec_TSL |
| TIP1-A_3981 | Protokollierung wichtiger TSL-spezifischer Ereignisse: Angaben | gemSpec_TSL |
| TIP1-A_3982 | Aufbewahrungsfrist für Protokolldaten | gemSpec_TSL |
| TIP1-A_3983 | Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten | gemSpec_TSL |
| TIP1-A_3984 | Archivierung: Relevante Daten | gemSpec_TSL |
| TIP1-A_3985 | Dokumentationspflicht für Prozesse zum Schlüsselwechsel | gemSpec_TSL |
| TIP1-A_3986 | Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung | gemSpec_TSL |
| TIP1-A_3987 | Herausgabe des Schlüsselmaterials | gemSpec_TSL |
| TIP1-A_3988 | Bewilligung der Herausgabe der Schlüsselmaterials | gemSpec_TSL |
| TIP1-A_3990 | Fortbestand von Archiven und die Abrufmöglichkeit aller TSL-Dateien und Zertifikate | gemSpec_TSL |
| TIP1-A_3993 | TSL-Signer-CA offline | gemSpec_TSL |
| TIP1-A_3995 | Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren | gemSpec_TSL |
| TIP1-A_3996 | Sicherheitsniveau bei der Generierung von Signaturschlüsseln | gemSpec_TSL |

| | | |
|-------------|--|-------------|
| TIP1-A_3997 | Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln | gemSpec_TSL |
| TIP1-A_3998 | Unterstützung des sicheren Löschen von Schlüsseln durch HSM | gemSpec_TSL |
| TIP1-A_3999 | Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip | gemSpec_TSL |
| TIP1-A_4000 | Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip | gemSpec_TSL |
| TIP1-A_4001 | Protokollierung der HSM-Nutzung | gemSpec_TSL |
| TIP1-A_4002 | Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln | gemSpec_TSL |
| TIP1-A_4003 | Anlass für den Wechsel von Schlüsselpaaren | gemSpec_TSL |
| TIP1-A_4005 | Sicherung des privaten Schlüssels | gemSpec_TSL |
| TIP1-A_4006 | Verwendung von privaten Schlüsseln | gemSpec_TSL |
| TIP1-A_4007 | Vorgaben an HSM-Funktionalität | gemSpec_TSL |
| TIP1-A_4008 | Speicherung und Auswahl von Schlüsselpaaren im HSM | gemSpec_TSL |
| TIP1-A_4010 | Vorgaben an die Prüftiefe der Evaluierung eines HSM | gemSpec_TSL |
| TIP1-A_4012 | Hinterlegung des privaten Schlüssels | gemSpec_TSL |
| TIP1-A_4016 | Maximale Gültigkeitsdauer des TSL-Signer-Zertifikats | gemSpec_TSL |
| TIP1-A_4017 | Sichere Übermittlung von Aktivierungsdaten | gemSpec_TSL |
| TIP1-A_4018 | Konformität zum betreiberspezifischen Sicherheitskonzept | gemSpec_TSL |
| TIP1-A_4019 | Härtung von Betriebssystemen | gemSpec_TSL |
| TIP1-A_4026 | Service Level | gemSpec_TSL |
| TIP1-A_4051 | Auftrag für Schlüsselerzeugung TSL-Signer-CA und OCSP-Responder | gemSpec_TSL |
| TIP1-A_4077 | Organisatorische Trennung für OCSP | gemSpec_TSL |
| TIP1-A_4078 | Sperrantrag | gemSpec_TSL |
| TIP1-A_4079 | Verfahren für Sperrung TSL-Signer-Zertifikat | gemSpec_TSL |
| TIP1-A_4439 | Schnittstelle I_TSL-Management für Test (TU) | gemSpec_TSL |

| | | |
|-------------|---|-------------|
| TIP1-A_4440 | Konzept Prozess für Schlüsselpaargenerierung und Zertifizierung | gemSpec_TSL |
| TIP1-A_4441 | Konzept Zertifikatswechsel | gemSpec_TSL |
| TIP1-A_4442 | Auftrag für Schlüsselerzeugung TSL-Signer | gemSpec_TSL |
| TIP1-A_4443 | TSL-Zertifikate für Test- und Referenzzwecke | gemSpec_TSL |
| TIP1-A_4446 | Trennung von Komponenten zwischen PU und TU-/RU-PKI | gemSpec_TSL |
| TIP1-A_4852 | TI-Vertrauensankerwechsel, Konzept | gemSpec_TSL |
| TIP1-A_5382 | Zugang zu HSM-Systemen im Vier-Augen-Prinzip | gemSpec_TSL |
| TIP1-A_6756 | BNetzA-VL-Signer-Zertifikate in TSL aufnehmen und entfernen | gemSpec_TSL |
| TIP1-A_6757 | Periodisches Aktualisieren der BNetzA-VL | gemSpec_TSL |
| TIP1-A_6758 | Prüfen und Bereitstellen der BNetzA-VL auf dem TSL-Dienst | gemSpec_TSL |
| TIP1-A_6769 | Gesichertes Herunterladen von Dateien der BNetzA | gemSpec_TSL |

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 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_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_5555 | Unverzögliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen | gemSpec_DS_Anbieter |
| GS-A_5556 | Unverzögliche 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_5624 | Auditrechte der gematik zur Informationssicherheit | gemSpec_DS_Anbieter |
| 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 |
| 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 | TLS-Klient zur Störungsampel oder zum SM (Zertifikatsprüfung) | gemSpec_Krypt |
| GS-A_5581 | "TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI) | gemSpec_Krypt |

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

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

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

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" | 17 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ... | 24 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" | 29 |

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 |