

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Produkttypsteckbrief**

*Prüfvorschrift*

## **Trust Service Provider X.509 nonQES – Komponentenzertifikate**

Produkttyp Version: 1.10.2-0  
Produkttyp Status: freigegeben

Version: 1.0.2  
Revision: 341174  
Stand: 19.02.2021  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_X509\_TSP\_nonQES\_Komp\_PTV\_1.10.2-0

## 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_X.509_TSP_nonQES_Komp_PTV1.0.0]   |
| 1.1.0             | Losübergreifende Synchronisation                | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.1.0]   |
| 1.2.0             | P11-Änderungsliste                              | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.2.0]   |
| 1.3.0             | P12-Änderungsliste                              | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.3.0]   |
|                   | Änderungen aus Errata 1.4.3 und 1.4.6 eingefügt |   |
| 1.6.0             | Aufnahme der Änderungen für KOM-LE              | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.6.0]   |
| 1.7.0             | OPB1 Anpassung                                  | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.7.0]   |
| 1.7.1             | R1.6.3 Anpassung                                | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.7.1]   |
| 1.7.1-0           | Anpassung auf Releasestand 1.6.3                | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.7.1-0] |
| 1.8.0-0           | Anpassung auf Releasestand 1.6.4                | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.8.0-0] |
| 1.8.0-1           | Errata 1.6.4-2                                  | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.8.0-1] |

|          |                                       |  |
|----------|---------------------------------------|--|
| 1.8.0-2  | Errata 1.6.4-3                        | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.8.0-2]  |
| 1.8.1-0  | Anpassung an<br>Releasestand<br>2.1.2 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.8.1-0]  |
| 1.8.2-0  | Anpassung an<br>Releasestand<br>2.1.3 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.8.2-0]  |
| 1.9.0-0  | Anpassung an<br>Releasestand<br>3.0.0 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.9.0-0]  |
| 1.10.0-0 | Anpassung an<br>Releasestand<br>3.1.0 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.10.0-0] |
| 1.10.1-0 | Anpassung an<br>Releasestand<br>3.1.2 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.10.1-0] |
| 1.10.2-0 | Anpassung an<br>Releasestand<br>4.0.0 | [gemProdT_X.509_TSP_nonQES_Komp_PTV1.10.2-0] |

### Historie Produkttypsteckbrief

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

| Version | Stand    | Kap. | Grund der Änderung, besondere Hinweise | Bearbeiter |
|---------|----------|------|--|------------|
| 1.0.0   | 30.06.20 |      | freigegeben                            | gematik    |
| 1.0.1   | 06.07.20 |      | GS-A_4147 und GS-A_4148 entfernt       | gematik    |
| 1.0.2   | 19.02.21 | 2    | Releasestand 4.0.2                     | gematik    |

---

## Inhaltsverzeichnis

---

|  |           |
|--|-----------|
| <b>1 Einführung .....</b>  | <b>5</b>  |
| <b>1.1 Zielsetzung und Einordnung des Dokumentes .....</b>                               | <b>5</b>  |
| <b>1.2 Zielgruppe .....</b>  | <b>5</b>  |
| <b>1.3 Geltungsbereich .....</b>   | <b>5</b>  |
| <b>1.4 Abgrenzung des Dokumentes .....</b>   | <b>6</b>  |
| <b>1.5 Methodik .....</b>  | <b>6</b>  |
| <b>2 Dokumente .....</b>   | <b>7</b>  |
| <b>3 Blattanforderungen.....</b>   | <b>8</b>  |
| <b>3.1 Anforderungen zur funktionalen Eignung .....</b>                                  | <b>8</b>  |
| 3.1.1 Produkttest/Produktübergreifender Test .....                                       | 8         |
| 3.1.2 Herstellererklärung funktionale Eignung .....                                      | 14        |
| <b>3.2 Anforderungen zur sicherheitstechnischen Eignung .....</b>                        | <b>22</b> |
| 3.2.1 CC-Evaluierung.....  | 22        |
| 3.2.2 Sicherheitsgutachten .....   | 22        |
| 3.2.3 Herstellererklärung sicherheitstechnische Eignung .....                            | 27        |
| <b>3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung .....</b> | <b>28</b> |
| <b>4 Produkttypspezifische Merkmale .....</b>  | <b>29</b> |
| <b>5 Anhang A – Verzeichnisse.....</b>   | <b>30</b> |
| <b>5.1 Abkürzungen .....</b>   | <b>30</b> |
| <b>5.2 Tabellenverzeichnis .....</b>   | <b>30</b> |
| <b>5.3 Referenzierte Dokumente.....</b>  | <b>30</b> |

---

## **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 Trust Service Provider X.509 nonQES – Komponentenzertifikate 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 Trust Service Provider X.509 nonQES – Komponentenzertifikate-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_OM          | Übergreifende Spezifikation Operations und Maintenance   | 1.14.0   |
| gemSpec_Net         | Übergreifende Spezifikation Netzwerk   | 1.4820.0 |
| gemSpec_PKI         | Übergreifende Spezifikation – Spezifikation PKI  | 2.910.02 |
| gemSpec_ServiceMon  | Spezifikation Service Monitoring   | 1.5.0    |
| gemSpec_X_509_TSP   | Spezifikation Trust Service Provider X.509   | 1.167.0  |
| gemSpec_Perf        | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform                              | 2.142.01 |
| gemSpec_Krypt       | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.179.0  |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter                         | 1.23.0   |
| gemKPT_Test         | Testkonzept der TI   | 2.78.0   |
| gemRL_TSL_SP_CP     | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL             | 2.67.0   |
| gemSpec_OID         | Spezifikation Festlegung von OIDs  | 3.810.0  |

### 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) |
|-----------|---|-------------------|
| GS-A_4178 | Standardkonforme Namensvergabe in Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4179 | Format von E-Mail-Adressen in Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4208 | Ausgabe von Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4213 | Zulässige Nutzungsarten   | gemRL_TSL_SP_CP   |
| GS-A_4225 | Festlegung eines Sperrberechtigten für Endanwenderzertifikate                         | gemRL_TSL_SP_CP   |
| GS-A_4228 | Unverzögliche Bearbeitung eines Sperrantrags  | gemRL_TSL_SP_CP   |
| GS-A_4303 | Festlegung der Schlüsselverwendung (keyUsage)   | gemRL_TSL_SP_CP   |
| GS-A_4333 | Informationspflicht gegenüber Antragsteller bei Sperrung eines Komponentenzertifikats | gemRL_TSL_SP_CP   |
| GS-A_4336 | Sperranträge der gematik für Komponentenzertifikate                                   | gemRL_TSL_SP_CP   |
| GS-A_4345 | Automatisierte Zertifikatsanträge für Komponentenzertifikate                          | gemRL_TSL_SP_CP   |
| GS-A_4348 | Verbot der Erneuerung von Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4352 | Maximale Gültigkeitsdauer eines Endbenutzerzertifikats                                | gemRL_TSL_SP_CP   |
| GS-A_4395 | Benachrichtigung des Zertifikatsnehmer  | gemRL_TSL_SP_CP   |
| GS-A_4906 | Zuordnung von Schlüsseln zu Identitäten   | gemRL_TSL_SP_CP   |
| GS-A_4911 | CP-Test, Standardkonforme Namensvergabe in Testzertifikaten                           | gemRL_TSL_SP_CP   |
| GS-A_4919 | CP-Test, Testkennzeichen in Testzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4926 | CP-Test, Policy von Testzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4931 | CP-Test, Maximale Gültigkeitsdauer von Testzertifikaten                               | gemRL_TSL_SP_CP   |
| A_17124   | TLS-Verbindungen (ECC-Migration)  | gemSpec_Krypt     |
| GS-A_4384 | TLS-Verbindungen  | gemSpec_Krypt     |



| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz) |
|--------------|---|-------------------|
| GS-A_5131    | Hash-Algorithmus bei OCSP/CertID  | gemSpec_Krypt     |
| GS-A_5339    | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität   | 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_4445-01 | OID-Festlegung für Zertifikatstypen   | gemSpec_OID       |
| GS-A_4446-02 | OID-Festlegung für technische Rollen  | 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_15172      | Umsetzung Zertifikatsprofil C.FD.SIG  | gemSpec_PKI       |
| A_15591      | Umsetzung Zertifikatsprofil C.FD.AUT  | gemSpec_PKI       |
| A_15676      | Reihenfolge der Elemente im SubjectDN von X.509-Zertifikaten  | gemSpec_PKI       |
| A_16213      | Umsetzung Zertifikatsprofil C.FD.ENC  | 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       |

| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz) |
|--------------|--|-------------------|
| A_17690      | Nutzung der Hash-Datei für TSL (ECC-Migration)                                     | 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       |
| A_17844      | Umsetzung Zertifikatsprofil C.SGD-HSM.AUT  | 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_4604    | Umsetzung Zertifikatsprofil C.SMKT.AUT   | gemSpec_PKI       |
| GS-A_4608    | Statusprüfung von Konnektorzertifikaten  | gemSpec_PKI       |
| GS-A_4609    | Umsetzung Zertifikatsprofil C.NK.VPN   | gemSpec_PKI       |
| GS-A_4610    | Umsetzung Zertifikatsprofil C.AK.AUT   | gemSpec_PKI       |
| GS-A_4611    | Umsetzung Zertifikatsprofil C.SAK.AUT  | gemSpec_PKI       |
| GS-A_4613    | Umsetzung Zertifikatsprofil C.VPNK.VPN   | gemSpec_PKI       |
| GS-A_4615    | Umsetzung Zertifikatsprofil C.ZD.TLS-S   | gemSpec_PKI       |
| GS-A_4617    | Umsetzung Zertifikatsprofil C.FD.TLS-C   | gemSpec_PKI       |
| GS-A_4618    | Umsetzung Zertifikatsprofil C.FD.TLS-S   | 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_4669    | Umsetzung Statusprüfdienst   | gemSpec_PKI       |

| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz) |
|--------------|--|-------------------|
| GS-A_4674-01 | OCSP-Requests gemäß Standards  | gemSpec_PKI       |
| GS-A_4676-01 | OCSP-Responses gemäß Standards                                       | 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_4693-01 | Statusprüfdienst – Positive Statement                                | gemSpec_PKI       |
| GS-A_4694    | Betrieb von OCSP-Responder für Test-PKI-CAs                          | gemSpec_PKI       |
| GS-A_4705-01 | Verarbeitung von Sonderzeichen in PKI-Komponenten                    | gemSpec_PKI       |
| GS-A_4706    | Vorgaben zu SubjectDN von CA- und OCSP-Zertifikaten                  | gemSpec_PKI       |
| GS-A_4714-01 | Kodierung der Attribute in X.509-Zertifikaten                        | gemSpec_PKI       |
| GS-A_4715-01 | Maximale Stringlänge der Attribute im SubjectDN                      | gemSpec_PKI       |
| GS-A_4716    | Umgang mit überlangen Organisationsnamen im SubjectDN                | gemSpec_PKI       |
| GS-A_4717-01 | TI-spezifische Vorgabe zur Nutzung der Extension Admission           | gemSpec_PKI       |
| GS-A_4718    | TI-spezifische Vorgabe zur Nutzung der Extension CertificatePolicies | gemSpec_PKI       |
| GS-A_4719    | TI-spezifische Vorgabe zur Nutzung der Extension SubjectAltNames     | gemSpec_PKI       |
| GS-A_4722    | Belegung der Felder professionInfos                                  | gemSpec_PKI       |
| GS-A_4724    | Komplettsperre aller Zertifikate einer Karte                         | gemSpec_PKI       |
| GS-A_4725    | Eindeutiger SubjectDN durch serialNumber                             | gemSpec_PKI       |
| GS-A_4726    | Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs     | gemSpec_PKI       |
| GS-A_4741    | Umsetzung Zertifikatsprofil C.GEM.OCSP                               | 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_4830    | Umsetzung Zertifikatsprofil C.VPNK.VPN-SIS                           | gemSpec_PKI       |
| GS-A_4898    | TSL-Grace-Period einer TSL   | gemSpec_PKI       |
| GS-A_4899    | TSL Update-Prüfintervall   | gemSpec_PKI       |
| GS-A_4936    | Attribute der CRL-Signer-Zertifikate                                 | gemSpec_PKI       |
| GS-A_4937    | Ableitung des CRL-Signer-Zertifikates                                | gemSpec_PKI       |
| GS-A_4939    | Umsetzung Zertifikatsprofil C.GEM.CRL                                | gemSpec_PKI       |

| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz)  |
|--------------|---|--------------------|
| GS-A_4957-01 | Beschränkungen OCSP-Request   | gemSpec_PKI        |
| GS-A_5066-01 | Indirekte CRL gemäß Standards   | gemSpec_PKI        |
| GS-A_5077    | FQDN-Prüfung beim TLS-Handshake   | gemSpec_PKI        |
| GS-A_5090    | Statusprüfdienst – Keine Angabe von Sperrgründen  | gemSpec_PKI        |
| GS-A_5280    | Umsetzung Zertifikatsprofil C.CM.TLS-CS   | gemSpec_PKI        |
| GS-A_5336    | Zertifikatsprüfung nach Ablauf TSL-Graceperiod  | gemSpec_PKI        |
| GS-A_5513    | Wahl des Signaturalgorithmus für Zertifikate  | gemSpec_PKI        |
| GS-A_5516    | Schlüsselgenerationen der CRL für Zertifikate des VPN-Zugangsdienstes   | gemSpec_PKI        |
| GS-A_5517    | Schlüsselgenerationen der OCSP-Signer-Zertifikate   | gemSpec_PKI        |
| A_14502      | Performance – CRL-Dienst – Last und Parallele Downloads   | gemSpec_Perf       |
| A_14936      | Performance - Störungssampel - Ereignisnachricht bei Ausfall zentrale Dienste   | gemSpec_Perf       |
| A_18013      | Performance – TSP – Provisioning/Revocation – Bearbeitungszeit  | 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_4160    | Performance – OCSP-Responder – Performance Reporting – Daten nach Zertifikatstyp  | 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 |
| A_14621      | Gültigkeitsdauer OCSP-Antworten VPNK-CA   | gemSpec_X.509_TSP  |
| A_14622      | Caching OCSP-Antworten VPNK-CA  | gemSpec_X.509_TSP  |
| TIP1-A_3559  | Schnittstellen TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate                               | gemSpec_X.509_TSP  |
| TIP1-A_3605  | Registrierungsdienst für Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate                                       | gemSpec_X.509_TSP  |
| TIP1-A_3607  | Request-Inhalte   | gemSpec_X.509_TSP  |
| TIP1-A_3609  | Überprüfung Hersteller, Anbieter und TSP-X.509 nonQES zu Produktangaben   | gemSpec_X.509_TSP  |
| TIP1-A_3612  | Erstellung von Zertifikaten   | gemSpec_X.509_TSP  |

| Afo-ID      | Afo-Bezeichnung  | Quelle (Referenz) |
|-------------|--|-------------------|
| TIP1-A_3615 | Ausstellung von Zertifikaten nach Widerruf eines Hersteller oder Anbieters   | gemSpec_X.509_TSP |
| TIP1-A_3620 | Technische Umsetzung Registrierungsdienst TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat  | gemSpec_X.509_TSP |
| TIP1-A_3621 | Zertifikatsmanagementprotokolle des Registrierungsdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate | gemSpec_X.509_TSP |
| TIP1-A_3623 | Eindeutigkeit des Zertifikats für den Produkttyp gSMC-KT   | gemSpec_X.509_TSP |
| TIP1-A_3647 | Rückmeldung zur Sperrung an den Antragsteller  | gemSpec_X.509_TSP |
| TIP1-A_3651 | Eingangsdaten zur Identifizierung des zu sperrenden Zertifikats  | gemSpec_X.509_TSP |
| TIP1-A_3654 | Umsetzung der Schnittstelle zur Sperrung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten                  | gemSpec_X.509_TSP |
| TIP1-A_3886 | OCSP-Adresse im X.509-Zertifikate  | gemSpec_X.509_TSP |
| TIP1-A_4240 | professionItem und professionOID für Komponenten- und Signerzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_4242 | Signierung des Test-nonQES-X.509-Zertifikats   | gemSpec_X.509_TSP |
| TIP1-A_4244 | Unmittelbare Ausführung der Sperrung für Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate                      | gemSpec_X.509_TSP |
| TIP1-A_4246 | Erzeugung einer CRL für Zertifikate von VPN-Zugangsdiensten  | gemSpec_X.509_TSP |
| TIP1-A_4247 | Bereitstellung der Sperrinformationen per CRL  | gemSpec_X.509_TSP |
| TIP1-A_4248 | CRL im Internet  | gemSpec_X.509_TSP |
| TIP1-A_4430 | I_Cert_Provisioning::provide_Certificate:SEND_REQUEST  | gemSpec_X.509_TSP |
| TIP1-A_4431 | Cert_Provisioning::provide_Certificate: GET_CERTIFICATE  | gemSpec_X.509_TSP |
| TIP1-A_4432 | I_Cert_Revocation::revoke_Certificate  | gemSpec_X.509_TSP |
| TIP1-A_4433 | I_Cert_Revocation::revoke_Certificate:SEND_REVOCATE_DATA   | gemSpec_X.509_TSP |
| TIP1-A_4466 | I_Cert_Provisioning::provide_Certificate: AUTHENTICATE_REQUESTOR   | gemSpec_X.509_TSP |
| TIP1-A_4469 | Technische Umsetzung Sperrdienst TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate          | gemSpec_X.509_TSP |
| TIP1-A_4470 | Zertifikatsmanagementprotokolle des Sperrdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate          | gemSpec_X.509_TSP |
| TIP1-A_5097 | Zertifikatsbeantragung über SOAP-Schnittstelle   | gemSpec_X.509_TSP |
| TIP1-A_5098 | Zertifikatsbeantragung über Web-Portal   | gemSpec_X.509_TSP |
| TIP1-A_5099 | I_Cert_Revocation::revoke_Certificate: AUTHENTICATE_REQUESTOR  | gemSpec_X.509_TSP |
| TIP1-A_5100 | I_Cert_Revocation::revoke_Certificate: GET_CERTIFICATE_STATUS  | gemSpec_X.509_TSP |
| TIP1-A_5101 | Zertifikatssperrung über Web-Schnittstelle   | gemSpec_X.509_TSP |
| TIP1-A_5102 | Zertifikatssperrung über Web-Portal  | gemSpec_X.509_TSP |

| Afo-ID                  | Afo-Bezeichnung  | Quelle (Referenz)       |
|-------------------------|--|-------------------------|
| <del>GS-A_4660-01</del> | <del>TUC_PKI_009: Rollenermittlung</del>                       | <del>gemSpec_PKI</del>  |
| <del>GS-A_4445</del>    | <del>OID-Festlegung für Zertifikatstypen</del>                 | <del>gemSpec_OID</del>  |
| <del>GS-A_4446-01</del> | <del>OID-Festlegung für technische Rollen</del>                | <del>gemSpec_OID</del>  |
| <del>GS-A_4149-01</del> | <del>Performance – Reporting-Daten in Performance-Report</del> | <del>gemSpec_Perf</del> |

### 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_2805    | Zeitnahe Anpassung von Produktkonfigurationen                             | 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_6517-01 | Eigenverantwortlicher Test: TBI   | gemKPT_Test       |
| TIP1-A_6518    | Eigenverantwortlicher Test: TDI   | gemKPT_Test       |
| TIP1-A_6519    | Eigenverantwortlicher Test: Hersteller und Anbieter                       | gemKPT_Test       |
| TIP1-A_6523    | Zulassungstest: Hersteller und Anbieter                                   | gemKPT_Test       |
| TIP1-A_6524-01 | Testdokumentation gemäß Vorlagen  | gemKPT_Test       |
| TIP1-A_6526    | Produkttypen: Bereitstellung  | gemKPT_Test       |
| TIP1-A_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       |

| Afo-ID      | Afo-Bezeichnung   | Quelle (Referenz) |
|-------------|---|-------------------|
| 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_17860     | OCSP-Statusauskunft bei Übernahme durch einen anderen TSP-X.509 nonQES                                      | gemRL_TSL_SP_CP   |
| A_17861     | Aufnahme der OCSP- und CRL-Signerzertifikate der TI in die TSL  | gemRL_TSL_SP_CP   |
| GS-A_4173   | Erbringung von Verzeichnisdienstleistungen  | gemRL_TSL_SP_CP   |
| GS-A_4174   | Veröffentlichung von CA- und Signer-Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4175   | Veröffentlichungspflicht für kritische Informationen  | gemRL_TSL_SP_CP   |
| GS-A_4176   | Mitteilungspflicht bei Änderungen   | gemRL_TSL_SP_CP   |
| GS-A_4177   | Zugriffskontrolle auf Verzeichnisse   | gemRL_TSL_SP_CP   |
| GS-A_4180   | Gestaltung der Struktur der Verzeichnisdienste  | gemRL_TSL_SP_CP   |
| GS-A_4181   | Eindeutigkeit der Namensform des Zertifikatsnehmers   | gemRL_TSL_SP_CP   |
| GS-A_4183   | Kennzeichnung von maschinen-, rollenbezogenen oder pseudonymisierten (nicht personenbezogenen) Zertifikaten | gemRL_TSL_SP_CP   |
| GS-A_4185   | Unterscheidung von Zertifikaten   | gemRL_TSL_SP_CP   |
| GS-A_4186   | Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer                                    | gemRL_TSL_SP_CP   |
| GS-A_4188   | Zuverlässige Identifizierung und vollständige Prüfung der Antragsdaten                                      | gemRL_TSL_SP_CP   |
| GS-A_4190   | Regelung für die Berechtigung zur Antragstellung  | gemRL_TSL_SP_CP   |
| GS-A_4192   | Prüfung der Berechtigung zur Antragstellung auf Schlüsselerneuerung   | gemRL_TSL_SP_CP   |
| GS-A_4195   | Schriftform für Aufnahme eines Zertifikats in die TSL   | gemRL_TSL_SP_CP   |
| GS-A_4199   | Berechtigung für Beantragung von CA-Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4201   | Dokumentation des Registrierungsprozesses   | gemRL_TSL_SP_CP   |
| GS-A_4202   | Identifikation des Zertifikatsnehmers im Rahmen der Registrierung   | gemRL_TSL_SP_CP   |
| GS-A_4203   | Dokumentationspflichten für die Beantragung von Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4207   | Vorgaben für die Ausgabe von Endnutzerzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4209   | Sicherstellung der Verbindung von Zertifikatsnehmer und privatem Schlüssel                                  | gemRL_TSL_SP_CP   |
| GS-A_4210   | Dokumentation der Annahme eines Zertifikatsantrags und der sicheren Ausgabe des Zertifikats                 | gemRL_TSL_SP_CP   |
| GS-A_4211   | Bereitstellung von CA-Zertifikaten bei Aufnahme in die TSL  | gemRL_TSL_SP_CP   |
| GS-A_4212   | Verwendung des privaten Schlüssels durch den Zertifikatsnehmer  | gemRL_TSL_SP_CP   |



| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz) |
|--------------|--|-------------------|
| GS-A_4214    | Veröffentlichung der öffentlichen Schlüssel durch den TSP-X.509 nonQES             | gemRL_TSL_SP_CP   |
| GS-A_4215    | Bedingungen für eine Zertifizierung nach Schlüsselerneuerung                       | gemRL_TSL_SP_CP   |
| GS-A_4218    | Beschreibung der Bedingungen für die Sperrung eines Anwenderzertifikats            | gemRL_TSL_SP_CP   |
| GS-A_4219-01 | Sperrung von Anwenderzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4221    | Anzeige der Kompromittierung des privaten Signaturschlüssels                       | gemRL_TSL_SP_CP   |
| GS-A_4226    | Verfahren für einen Sperrantrag  | gemRL_TSL_SP_CP   |
| GS-A_4227    | Dokumentation der Fristen für einen Sperrantrag                                    | gemRL_TSL_SP_CP   |
| GS-A_4229    | Methoden zum Prüfen von Sperrinformationen   | gemRL_TSL_SP_CP   |
| GS-A_4230    | Gewährleistung der Online-Verfügbarkeit von Sperrinformationen                     | gemRL_TSL_SP_CP   |
| GS-A_4231    | Anforderungen zur Online-Prüfung von Sperrinformationen                            | gemRL_TSL_SP_CP   |
| GS-A_4238    | Funktionsbeschreibung des Statusabfragedienstes                                    | gemRL_TSL_SP_CP   |
| GS-A_4241    | Sperrung von Zertifikaten bei Kündigung durch den Zertifikatsnehmer                | gemRL_TSL_SP_CP   |
| GS-A_4242    | Dokumentationspflicht für Prozesse der Schlüsselhinterlegung                       | gemRL_TSL_SP_CP   |
| GS-A_4245    | Anzeige von Änderung an der Gesellschafterstruktur des Betreibers                  | gemRL_TSL_SP_CP   |
| GS-A_4248    | Bereitstellung der Protokollierungsdaten   | gemRL_TSL_SP_CP   |
| GS-A_4250    | Verwendung des Backup-HSM gemäß Vier-Augen-Prinzip                                 | gemRL_TSL_SP_CP   |
| GS-A_4251    | Backup-Konzept   | gemRL_TSL_SP_CP   |
| GS-A_4252    | Besetzung von Rollen und Informationspflichten                                     | gemRL_TSL_SP_CP   |
| GS-A_4254    | Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips                              | gemRL_TSL_SP_CP   |
| GS-A_4256    | Zugang zu Systemen für die Zertifikatserzeugung                                    | gemRL_TSL_SP_CP   |
| GS-A_4262    | Gewährleistung des Zugangs zur Betriebsstätte                                      | gemRL_TSL_SP_CP   |
| GS-A_4263    | Rollenunterscheidung im organisatorischen Konzept                                  | gemRL_TSL_SP_CP   |
| GS-A_4264    | Mitteilungspflicht für Zuordnung der Rollen  | gemRL_TSL_SP_CP   |
| GS-A_4265    | Obligatorische Rollen für sicherheitsrelevante Tätigkeiten                         | gemRL_TSL_SP_CP   |
| GS-A_4266    | Ausschluss von Rollenzuordnungen   | gemRL_TSL_SP_CP   |
| GS-A_4267    | Rollenaufteilung auf Personengruppen   | gemRL_TSL_SP_CP   |
| GS-A_4269    | Einsicht in Dokumente für Mitarbeiter  | gemRL_TSL_SP_CP   |
| GS-A_4276    | Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung                       | gemRL_TSL_SP_CP   |
| GS-A_4277    | Anzeigepflicht bei Beendigung der Zertifizierungsdienstleistungen                  | gemRL_TSL_SP_CP   |
| GS-A_4278    | Maßnahmen zur Einstellung des Zertifizierungsbetriebs                              | gemRL_TSL_SP_CP   |
| GS-A_4281    | Fristen bei der Einstellung des Zertifizierungsbetriebs für einen TSP-X.509 nonQES | gemRL_TSL_SP_CP   |
| GS-A_4282    | Erforderliche Form bei Einstellung des Zertifizierungsbetriebs                     | gemRL_TSL_SP_CP   |



| Afo-ID    | Afo-Bezeichnung  | Quelle (Referenz) |
|-----------|--|-------------------|
| GS-A_4283 | Gültigkeit der Zertifikate bei Einstellung des Zertifizierungsbetriebs                                 | gemRL_TSL_SP_CP   |
| GS-A_4296 | Anlass für den Wechsel von Schlüsselpaaren   | gemRL_TSL_SP_CP   |
| GS-A_4297 | Behandlung einer Kompromittierung eines Schlüsselpaares  | gemRL_TSL_SP_CP   |
| GS-A_4299 | Zulassung/Abnahme und Aufnahme in den Vertrauensraum der TI  | gemRL_TSL_SP_CP   |
| GS-A_4300 | Zweckbindung von Schlüsselpaaren   | gemRL_TSL_SP_CP   |
| GS-A_4302 | Transportmedium für die Übergabe des privaten Schlüssels eines Schlüsselpaares                         | gemRL_TSL_SP_CP   |
| GS-A_4318 | Maßnahmen zur Beurteilung der Systemsicherheit   | gemRL_TSL_SP_CP   |
| GS-A_4319 | Prüfpflichten vor Nutzung neuer Software im Wirkbetrieb  | gemRL_TSL_SP_CP   |
| GS-A_4321 | Bereitstellung eines Certificate Policy Disclosure Statements  | gemRL_TSL_SP_CP   |
| GS-A_4322 | Zusicherung der Dienstqualität   | gemRL_TSL_SP_CP   |
| GS-A_4323 | Wahrung der Vertraulichkeit  | gemRL_TSL_SP_CP   |
| GS-A_4324 | Zusicherung der Dienstgüte   | gemRL_TSL_SP_CP   |
| GS-A_4325 | Zweckbindung von Zertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4326 | Dokumentationspflicht für beschränkte Gültigkeit   | gemRL_TSL_SP_CP   |
| GS-A_4327 | Transparenz für Nachträge zum Certificate Policy Statement   | gemRL_TSL_SP_CP   |
| GS-A_4328 | Informationspflicht bei Änderung des CPS   | gemRL_TSL_SP_CP   |
| GS-A_4331 | Sicherstellungspflicht des Antragstellers eines Komponentenzertifikats                                 | gemRL_TSL_SP_CP   |
| GS-A_4332 | Dokumentation der Pflichten des Antragstellers eines Komponentenzertifikats                            | gemRL_TSL_SP_CP   |
| GS-A_4335 | Keine Sperrung eines Zertifikats für den Produkttyp gSMC-KT  | gemRL_TSL_SP_CP   |
| GS-A_4337 | Sonderregelung für die Sperrung von Komponentenzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4340 | Befristung von Sperranträgen für Komponentenzertifikate  | gemRL_TSL_SP_CP   |
| GS-A_4341 | Entfall der Verpflichtung für die Bereitstellung einer Statusprüfung bestimmter Komponentenzertifikate | gemRL_TSL_SP_CP   |
| GS-A_4344 | Sperrung von Komponentenzertifikate bei Schließung eines TSP-X.509 nonQES                              | gemRL_TSL_SP_CP   |
| GS-A_4349 | Obligatorische Gründe für die Sperrung eines selbst signierten Zertifikats eines TSP-X.509 nonQES      | gemRL_TSL_SP_CP   |
| GS-A_4394 | Dokumentation der Zertifikatsausgabeprozesse   | gemRL_TSL_SP_CP   |
| GS-A_4908 | CP-Test, Erfüllung der Certificate Policy für Testzertifikate zur Aufnahme in die Test-TSL             | gemRL_TSL_SP_CP   |
| GS-A_4909 | CP-Test, Erbringung von Verzeichnisdienstleistungen für Testzertifikate                                | gemRL_TSL_SP_CP   |
| GS-A_4910 | CP-Test, Zugriffskontrolle auf Verzeichnisse für Testzertifikate                                       | gemRL_TSL_SP_CP   |
| GS-A_4912 | CP-Test, Format von E-Mail-Adressen in Testzertifikaten  | gemRL_TSL_SP_CP   |
| GS-A_4913 | CP-Test, Gestaltung der Struktur der Verzeichnisdienste  | gemRL_TSL_SP_CP   |
| GS-A_4914 | CP-Test, Eindeutigkeit der Namensform des Zertifikatsnehmers   | gemRL_TSL_SP_CP   |

| Afo-ID    | Afo-Bezeichnung  | Quelle (Referenz) |
|-----------|--|-------------------|
| GS-A_4915 | CP-Test, Kein Bezug zu Echtdaten von Personen oder Organisationen  | gemRL_TSL_SP_CP   |
| GS-A_4917 | CP-Test, Kennzeichnung von maschinen-, rollenbezogenen oder pseudonymisierten (nicht personenbezogenen) Testzertifikaten | gemRL_TSL_SP_CP   |
| GS-A_4923 | CP-Test, Veröffentlichung von Testausstellerzertifikaten   | gemRL_TSL_SP_CP   |
| GS-A_4925 | CP-Test, Keine Verwendung von Echtdaten  | gemRL_TSL_SP_CP   |
| GS-A_4927 | CP-Test, Bereitstellung eines Sperrdienstes  | gemRL_TSL_SP_CP   |
| GS-A_4929 | CP-Test, Funktionsweise des Statusabfragedienst  | gemRL_TSL_SP_CP   |
| GS-A_4930 | CP-Test, Verfügbarkeit des Statusabfragedienstes   | gemRL_TSL_SP_CP   |
| GS-A_4933 | CP-Test, Zertifikatsprofile für Testzertifikate  | gemRL_TSL_SP_CP   |
| GS-A_5083 | Zertifikatsantragstellung im Vier-Augen-Prinzip  | gemRL_TSL_SP_CP   |
| GS-A_5084 | Zugang zu HSM-Systemen im Vier-Augen-Prinzip   | gemRL_TSL_SP_CP   |
| A_15590   | Zertifikatslaufzeit bei Erstellung von X.509-Zertifikaten mit RSA 2048 Bit   | gemSpec_Krypt     |
| A_17091   | ECC-Schlüsselkodierung   | gemSpec_Krypt     |
| A_17092   | RSA-Schlüssel Zertifikatserstellung, keine kleinen Primteiler und e ist prim   | gemSpec_Krypt     |
| A_17093   | RSA-Schlüssel Zertifikatserstellung, Entropie der Schlüsselkodierung   | gemSpec_Krypt     |
| A_17205   | Signatur der TSL: Signieren und Prüfen (ECC-Migration)   | gemSpec_Krypt     |
| A_17294   | TSP-X.509: Prüfung auf angreifbare (schwache) Schlüssel  | gemSpec_Krypt     |
| A_17775   | TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)  | gemSpec_Krypt     |
| GS-A_5518 | Prüfung Kurvenpunkte bei einer Zertifikatserstellung   | 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       |

| Afo-ID    | Afo-Bezeichnung   | Quelle (Referenz) |
|-----------|---|-------------------|
| GS-A_4759 | IPv4-Adressen Produkttyp zum SZZP   | gemSpec_Net       |
| GS-A_4805 | Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz                             | gemSpec_Net       |
| GS-A_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_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_17700   | TSL-Auswertung ServiceTypenidentifizier "unspecified"   | 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_4697 | PKI für Test- und Referenzumgebung  | gemSpec_PKI       |
| GS-A_4702 | Zentrale Aussteller-CA für nonQES-Zertifikate   | 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_4708 | Verwendung von Kennzeichen für Technische Rolle   | gemSpec_PKI       |
| GS-A_4721 | Beantragung Rollenattribute im X.509-Zertifikatsrequest   | gemSpec_PKI       |
| GS-A_4727 | PKI-Separierung von Test- und Produktivumgebung in der TI   | gemSpec_PKI       |
| GS-A_4730 | Eindeutige Identifizierung der CA-Zertifikate   | gemSpec_PKI       |

| Afo-ID      | Afo-Bezeichnung   | Quelle (Referenz)  |
|-------------|---|--------------------|
| GS-A_4731   | Attribute der CA-Zertifikate  | gemSpec_PKI        |
| GS-A_4735   | Namenskonvention für CA-Zertifikate   | gemSpec_PKI        |
| GS-A_4737   | Umsetzung nonQES-CA-Zertifikate   | 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_4828   | Vorgaben zur Bildung von nonQES-CA-Namen  | gemSpec_PKI        |
| GS-A_4935   | Eindeutige Identifizierung der CRL-Signer-Zertifikate   | gemSpec_PKI        |
| GS-A_5074   | Bereitstellung CRL und OCSP für Zertifikate des VPN-Zugangsdienstes                                     | gemSpec_PKI        |
| GS-A_5212   | Zentrale Aussteller-CA für VPN-Zugangsdienst-Zertifikate  | gemSpec_PKI        |
| GS-A_5337   | Größenbeschränkung von X.509 Zertifikaten auf Karten  | gemSpec_PKI        |
| GS-A_5511   | Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 nonQES  | gemSpec_PKI        |
| GS-A_5514   | Verwendung separater OCSP-Signer-Zertifikate  | gemSpec_PKI        |
| GS-A_5515   | Bezug separater CRL-Signer-Zertifikate  | gemSpec_PKI        |
| GS-A_5528   | Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 nonQES                                      | 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_4159   | Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast                                     | gemSpec_Perf       |
| GS-A_5028   | Performance – zentrale Dienste – Verfügbarkeit Produktivbetrieb   | 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_3547 | Erstellung einer Ausgabepolicy  | gemSpec_X.509_TSP  |
| TIP1-A_3555 | Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA                                | gemSpec_X.509_TSP  |
| TIP1-A_3597 | Eingangsprüfung Berechtigungsinformationen für Komponenten- und Signerzertifikate                       | gemSpec_X.509_TSP  |
| TIP1-A_3598 | Verbindliche Nutzung der Berechtigungsinformationen   | gemSpec_X.509_TSP  |
| TIP1-A_3599 | Registrierungsverfahren Antragsberechtigter   | gemSpec_X.509_TSP  |

| Afo-ID      | Afo-Bezeichnung   | Quelle (Referenz) |
|-------------|---|-------------------|
| TIP1-A_3601 | Regelung des Registrierungsverfahrens für Hersteller , Anbieter und TSP-X.509 nonQES  | gemSpec_X.509_TSP |
| TIP1-A_3603 | Überprüfung bei Registrierung der Antragsteller für Komponenten- und Signerzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3606 | Automatisierter Registrierungsdiens für Komponentenzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3608 | Überprüfung Zertifikatsantrag für Komponentenzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3611 | Eindeutige Zuordnung Zertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3613 | Widerruf der Registrierung von Antragsberechtigten  | gemSpec_X.509_TSP |
| TIP1-A_3614 | Widerrufsverfahren der Zertifikatsantragsberechtigung   | gemSpec_X.509_TSP |
| TIP1-A_3616 | Weiterleitung der Daten an den Registrierungsdiens des TSP-X.509  | gemSpec_X.509_TSP |
| TIP1-A_3618 | Umsetzung Registrierungsdiens für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate                                     | gemSpec_X.509_TSP |
| TIP1-A_3619 | Voraussetzungen zur Umsetzung Registrierungsdiens TSP-X.509 nonQES für Komponenten-, Signer, nonQES-HBA- und Organisationszertifikate | gemSpec_X.509_TSP |
| TIP1-A_3622 | Eindeutige Verbindung Zertifikatsnehmer und privater Schlüssel  | gemSpec_X.509_TSP |
| TIP1-A_3624 | Verwendung des Host- und Domänenname  | gemSpec_X.509_TSP |
| TIP1-A_3626 | Erstellung von X.509-Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikaten  | gemSpec_X.509_TSP |
| TIP1-A_3627 | Bereitstellung der Zertifikatsstatusinformationen der Komponenten- und Signerzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3629 | Umsetzung Erstellungsdiens für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten                                       | gemSpec_X.509_TSP |
| TIP1-A_3643 | Implementierung eines Sperrdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate                               | gemSpec_X.509_TSP |
| TIP1-A_3644 | Abgleich der Registrierungsdaten mit vorhandenen Daten aus der Berechtigungsinformation   | gemSpec_X.509_TSP |
| TIP1-A_3645 | Prüfung der Sperrberechtigung für Komponenten- und Signerzertifikate  | gemSpec_X.509_TSP |
| TIP1-A_3646 | Automatisierte Anlieferung und Bearbeitung von Sperranträgen für Komponenten- und Signerzertifikate                                   | gemSpec_X.509_TSP |
| TIP1-A_3648 | Angaben zur Identifizierung des zu sperrenden Zertifikats   | gemSpec_X.509_TSP |
| TIP1-A_3649 | Prüfungen bei Eingang eines Sperrantrags  | gemSpec_X.509_TSP |
| TIP1-A_3650 | Prüfung der Sperrantragsangaben   | gemSpec_X.509_TSP |
| TIP1-A_3652 | Regelungen zum Sperrprozess   | gemSpec_X.509_TSP |
| TIP1-A_3653 | Keine Bearbeitung von Sperranträgen bei nicht berechtigter Beantragung  | gemSpec_X.509_TSP |
| TIP1-A_3877 | Darstellung der Zusammenarbeit von Kartenherausgeber, Kartenhersteller und TSP-X.509 im Sicherheitskonzept                            | gemSpec_X.509_TSP |
| TIP1-A_3880 | Bestätigung Auflagen bei Widerruf der Zulassung   | gemSpec_X.509_TSP |
| TIP1-A_3883 | Sicherstellung TSP-X.509 OCSP-Responder und Sperrdienst bei nicht-sicherheitskritischen Incidents                                     | gemSpec_X.509_TSP |

| Afo-ID                  | Afo-Bezeichnung  | Quelle (Referenz)          |
|-------------------------|--|----------------------------|
| TIP1-A_3884             | Umgang mit nicht-sicherheitskritischen Incidents für nonQES-Personen- und Organisationszertifikate                                       | gemSpec_X.509_TSP          |
| TIP1-A_3887             | Verarbeitung von Anträgen bei einem nicht-sicherheitskritischen Incidents von X.509-Personen- und Organisationszertifikaten              | gemSpec_X.509_TSP          |
| TIP1-A_3889             | Festlegung des Registrierungsverfahrens  | gemSpec_X.509_TSP          |
| TIP1-A_3890             | Umgang mit nicht-sicherheitskritischen Incidents für Komponentenzertifikate  | gemSpec_X.509_TSP          |
| TIP1-A_3891             | Verarbeitung von Anträgen bei nicht-sicherheitskritischen Incidents von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten | gemSpec_X.509_TSP          |
| TIP1-A_3894             | Obligatorisch abzuleitende Sub-CAs unterhalb der gematikRoot-CA  | gemSpec_X.509_TSP          |
| TIP1-A_4248             | CRL im Internet  | gemSpec_X.509_TSP          |
| TIP1-A_4427             | Betrieb einer Test-TSP-X.509   | gemSpec_X.509_TSP          |
| TIP1-A_4429             | I_Cert_Provisioning::provide_Certificate   | gemSpec_X.509_TSP          |
| TIP1-A_4464             | Eingangsprüfung Berechtigungsinformationen für nonQES-HBA- und Organisationszertifikate  | gemSpec_X.509_TSP          |
| TIP1-A_4465             | Überprüfung bei Registrierung der Antragsteller für nonQES-HBA- und Organisationszertifikate   | gemSpec_X.509_TSP          |
| TIP1-A_4468             | Aktualisierung der CRL   | gemSpec_X.509_TSP          |
| TIP1-A_5376             | Erreichbarkeit des Sperrdienstes von TSP-X.509 nonQES und gematik Root-CA  | gemSpec_X.509_TSP          |
| <del>GS-A_4219</del>    | <del>Sperrung von Anwenderzertifikaten</del>   | <del>gemRL_TSL_SP_CP</del> |
| <del>GS-A_4149-01</del> | <del>Performance – Reporting Daten in Performance Report</del>   | <del>gemSpec_Perf</del>    |

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria ist nicht erforderlich.

### 3.2.2 Sicherheitsgutachten

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

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

| Afo-ID    | Afo-Bezeichnung   | Quelle (Referenz) |
|-----------|---|-------------------|
| GS-A_4173 | Erbringung von Verzeichnisdienstleistungen                        | gemRL_TSL_SP_CP   |
| GS-A_4191 | Einsatz interoperabler Systeme durch einen externen Dienstleister | gemRL_TSL_SP_CP   |

| Afo-ID    | Afo-Bezeichnung  | Quelle (Referenz) |
|-----------|--|-------------------|
| GS-A_4230 | Gewährleistung der Online-Verfügbarkeit von Sperrinformationen   | gemRL_TSL_SP_CP   |
| GS-A_4247 | Obligatorische Vorgaben für das Rollenkonzept  | gemRL_TSL_SP_CP   |
| GS-A_4249 | Standort für Backup-HSM  | gemRL_TSL_SP_CP   |
| GS-A_4255 | Nutzung des HSM im kontrollierten Bereich  | gemRL_TSL_SP_CP   |
| GS-A_4259 | Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung | gemRL_TSL_SP_CP   |
| GS-A_4260 | Manipulationsschutz veröffentlichter Daten   | gemRL_TSL_SP_CP   |
| GS-A_4261 | Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems                        | gemRL_TSL_SP_CP   |
| GS-A_4268 | Anforderungen an den Einsatz freier Mitarbeiter  | gemRL_TSL_SP_CP   |
| GS-A_4270 | Aufzeichnung von technischen Ereignissen   | gemRL_TSL_SP_CP   |
| GS-A_4271 | Aufzeichnung von organisatorischen Ereignissen   | gemRL_TSL_SP_CP   |
| GS-A_4272 | Aufbewahrungsfrist für sicherheitsrelevante Protokolldaten   | gemRL_TSL_SP_CP   |
| GS-A_4273 | Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten                            | gemRL_TSL_SP_CP   |
| GS-A_4274 | Archivierung von für den Zertifizierungsprozess relevanten Daten                                       | gemRL_TSL_SP_CP   |
| GS-A_4275 | Dokumentationspflicht für Prozesse zum Schlüsselwechsel  | gemRL_TSL_SP_CP   |
| GS-A_4276 | Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung   | gemRL_TSL_SP_CP   |
| GS-A_4279 | Fortbestand von Archiven und die Abrufmöglichkeit einer vollständigen Widerrufsliste                   | gemRL_TSL_SP_CP   |
| GS-A_4284 | Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren          | gemRL_TSL_SP_CP   |
| GS-A_4285 | Sicherheitsniveau bei der Generierung von Signaturschlüsseln   | gemRL_TSL_SP_CP   |
| GS-A_4287 | Sichere Aufbewahrung des privaten Schlüssels einer CA  | gemRL_TSL_SP_CP   |
| GS-A_4288 | Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln                                     | gemRL_TSL_SP_CP   |
| GS-A_4289 | Unterstützung des sicheren Löschen von Schlüsseln durch HSM  | gemRL_TSL_SP_CP   |
| GS-A_4290 | Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip                                    | gemRL_TSL_SP_CP   |
| GS-A_4291 | Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip                                       | gemRL_TSL_SP_CP   |
| GS-A_4292 | Protokollierung der HSM-Nutzung  | gemRL_TSL_SP_CP   |
| GS-A_4294 | Bedienung des Schlüsselgenerierungssystems   | gemRL_TSL_SP_CP   |
| GS-A_4295 | Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln                     | gemRL_TSL_SP_CP   |
| GS-A_4304 | Speicherung und Anwendung von privaten Schlüsseln  | gemRL_TSL_SP_CP   |
| GS-A_4305 | Ordnungsgemäße Sicherung des privaten Schlüssels   | gemRL_TSL_SP_CP   |
| GS-A_4306 | Verwendung von privaten Schlüsseln   | gemRL_TSL_SP_CP   |



| Afo-ID       | Afo-Bezeichnung   | Quelle (Referenz)   |
|--------------|---|---------------------|
| GS-A_4307    | Vorgaben an HSM-Funktionalität  | gemRL_TSL_SP_CP     |
| GS-A_4308    | Speicherung und Auswahl von Schlüsselpaaren im HSM  | gemRL_TSL_SP_CP     |
| GS-A_4309    | Verwendung von zertifizierten kryptographischen Modulen   | gemRL_TSL_SP_CP     |
| GS-A_4310    | Vorgaben an die Prüftiefe der Evaluierung eines HSM   | gemRL_TSL_SP_CP     |
| GS-A_4311    | Hinterlegung des privaten Signaturschlüssels  | gemRL_TSL_SP_CP     |
| GS-A_4312    | Aktivierung privater Schlüssel  | gemRL_TSL_SP_CP     |
| GS-A_4313    | Deaktivierung privater Schlüssel  | gemRL_TSL_SP_CP     |
| GS-A_4314    | Sichere Übermittlung von Aktivierungsdaten  | gemRL_TSL_SP_CP     |
| GS-A_4315    | Konformität zum betreiberspezifischen Sicherheitskonzept  | gemRL_TSL_SP_CP     |
| GS-A_4316    | Härtung von Betriebssystemen  | gemRL_TSL_SP_CP     |
| GS-A_4317    | Obligatorische Sicherheitsmaßnahmen   | gemRL_TSL_SP_CP     |
| GS-A_4339    | Autorisierung für die Sperrung von Komponentenzertifikaten  | gemRL_TSL_SP_CP     |
| GS-A_4342    | Verbot einer Schlüsselhinterlegung für Komponentenzertifikate   | gemRL_TSL_SP_CP     |
| GS-A_4343    | Unterstützung der Übergabe bei Schließung eines TSP-X.509 nonQES für Komponentenzertifikate                       | gemRL_TSL_SP_CP     |
| GS-A_4396    | Speicherung hinterlegter Root- und CA-Schlüssel   | gemRL_TSL_SP_CP     |
| GS-A_4925    | CP-Test, Keine Verwendung von Echtdaten   | gemRL_TSL_SP_CP     |
| 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 |



| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz)   |
|--------------|--|---------------------|
| 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_17294      | TSP-X.509: Prüfung auf angreifbare (schwache) Schlüssel  | 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_4362    | X.509-Identitäten für Verschlüsselungszertifikate  | gemSpec_Krypt       |
| GS-A_4367    | Zufallszahlengenerator   | gemSpec_Krypt       |
| GS-A_4368    | Schlüsselerzeugung   | gemSpec_Krypt       |
| GS-A_4384    | TLS-Verbindungen   | gemSpec_Krypt       |
| GS-A_4385    | TLS-Verbindungen, Version 1.2  | gemSpec_Krypt       |
| GS-A_4387    | TLS-Verbindungen, nicht Version 1.0  | gemSpec_Krypt       |
| GS-A_4388    | DNSSEC-Kontext   | gemSpec_Krypt       |
| GS-A_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_5518    | Prüfung Kurvenpunkte bei einer Zertifikatserstellung   | gemSpec_Krypt       |
| GS-A_4054    | Paketfilter Default Deny   | 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_4879    | DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern  | gemSpec_Net         |

| Afo-ID      | Afo-Bezeichnung   | Quelle (Referenz) |
|-------------|---|-------------------|
| GS-A_4641   | Initiale Einbringung TI-Vertrauensanker   | gemSpec_PKI       |
| GS-A_4748   | Initiale Einbringung TSL-Datei  | gemSpec_PKI       |
| TIP1-A_3548 | Schützenswerte Objekte  | gemSpec_X.509_TSP |
| TIP1-A_3549 | Vorgaben zum Schutzbedarf durch die gematik   | gemSpec_X.509_TSP |
| TIP1-A_3550 | Spezifische Erhöhung des Schutzbedarfs ist zulässig   | gemSpec_X.509_TSP |
| TIP1-A_3554 | Gesicherte interne Schnittstellen des TSP-X.509 QES und TSP-X.509 nonQES                    | gemSpec_X.509_TSP |
| TIP1-A_3555 | Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA                    | gemSpec_X.509_TSP |
| TIP1-A_3557 | Gesicherte externe Schnittstellen des TSP-X.509 nonQES                                      | gemSpec_X.509_TSP |
| TIP1-A_3660 | Trennung der TSP-X.509-Betriebsumgebungen   | gemSpec_X.509_TSP |
| TIP1-A_3881 | Schutzbedarf darf nicht verringert werden   | gemSpec_X.509_TSP |
| TIP1-A_4230 | Datenschutzgerechte Antrags- und Sperrprozesse  | gemSpec_X.509_TSP |
| TIP1-A_4231 | Löschung gespeicherter X.509-Zertifikate  | gemSpec_X.509_TSP |
| TIP1-A_4232 | Löschung von TSP-X.509 nonQES-Zertifikatsstatusinformationen, Zertifikats- und Sperranträge | gemSpec_X.509_TSP |
| TIP1-A_4234 | Protokollierungsverbot für OCSP-Anfragen  | gemSpec_X.509_TSP |
| TIP1-A_4235 | Fehlerprotokollierung   | gemSpec_X.509_TSP |
| TIP1-A_5087 | Berücksichtigung und Umsetzung übergeordneter Herausgeberpolicies                           | gemSpec_X.509_TSP |

Ein TSPs X.509 nonQES, der gleichzeitig eine VDA-Qualifizierung vorweist, kann ein reduziertes Sicherheitsgutachten vorlegen. Voraussetzung hierfür ist, dass der Anbieter

- ein qualifizierter Vertrauensdiensteanbieter für QES ist und die Konformität geeignet nachweist (z.B. mittels Qualifikationsbescheid der Bundesnetzagentur).
- erklärt, dass für die gegenständlichen Sicherheitsanforderungen der Betrieb des TSP X.509 nonQES äquivalent zum VDA-Bereich erfolgt.

Folgende Anforderungen müssen unter den o.g. Voraussetzungen nicht im Sicherheitsgutachten nachgewiesen werden:

**Tabelle 5: nicht nachzuweisende Anforderungen**

|           |           |           |              |              |
|-----------|-----------|-----------|--------------|--------------|
| GS-A_4173 | GS-A_4275 | GS-A_4305 | GS-A_2328-01 | GS-A_2329-01 |
| GS-A_4191 | GS-A_4276 | GS-A_4306 | GS-A_4980-01 | GS-A_2331-01 |
| GS-A_4230 | GS-A_4279 | GS-A_4307 | GS-A_4981-01 | GS-A_2332-01 |
| GS-A_3130 | GS-A_4284 | GS-A_4308 | GS-A_4982-01 | GS-A_3139    |
| GS-A_4249 | GS-A_4285 | GS-A_4309 | GS-A_4983-01 | GS-A_3141    |

|           |           |           |              |              |
|-----------|-----------|-----------|--------------|--------------|
| GS-A_4255 | GS-A_4287 | GS-A_4310 | GS-A_4984-01 | GS-A_3149    |
| GS-A_4259 | GS-A_4288 | GS-A_4311 | GS-A_3772-01 | TIP1-A_3548  |
| GS-A_4261 | GS-A_4289 | GS-A_4312 | GS-A_4367    | TIP1-A_3550  |
| GS-A_4268 | GS-A_4290 | GS-A_4313 | GS-A_4368    | TIP1-A_3554  |
| GS-A_4270 | GS-A_4291 | GS-A_4314 | GS-A_3737-01 | TIP1-A_4230  |
| GS-A_4271 | GS-A_4292 | GS-A_4315 | GS-A_3078    | TIP1-A_4235  |
| GS-A_4272 | GS-A_4294 | GS-A_4316 | GS-A_3753-01 | GS-A_2345-01 |
| GS-A_4273 | GS-A_4295 | GS-A_4317 | GS-A_3125    |              |
| GS-A_4274 | GS-A_4304 | GS-A_4906 | GS-A_2158-01 |              |

### 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 6: 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    | Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen                         | gemSpec_DS_Anbieter |
| GS-A_5556    | Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen                        | gemSpec_DS_Anbieter |
| GS-A_5559    | Bereitstellung Ergebnisse von Schwachstellenscans   | gemSpec_DS_Anbieter |
| GS-A_5560    | Entgegennahme und Prüfung von Meldungen der gematik   | gemSpec_DS_Anbieter |

| Afo-ID       | Afo-Bezeichnung  | Quelle (Referenz)   |
|--------------|--|---------------------|
| 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_15590      | Zertifikatslaufzeit bei Erstellung von X.509-Zertifikaten mit RSA 2048 Bit | gemSpec_Krypt       |
| A_17205      | Signatur der TSL: Signieren und Prüfen (ECC-Migration)                     | gemSpec_Krypt       |
| A_17294      | TSP-X.509: Prüfung auf angreifbare (schwache) Schlüssel                    | 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_5518    | Prüfung Kurvenpunkte bei einer Zertifikatserstellung                       | 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_4965    | Keine Suspendierung von X.509-Zertifikaten (außer für eGK)                 | 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**

| <b>Kürzel</b> | <b>Erläuterung</b>          |
|---------------|-----------------------------|
| Afo-ID        | Anforderungs-Identifikation |
| CC            | Common Criteria             |

### **5.2 Tabellenverzeichnis**

|  |    |
|--|----|
| Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion .....                            | 7  |
| Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" ..... | 8  |
| Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellereklärung" .....                     | 14 |
| Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ..            | 22 |
| Tabelle 5: nicht nachzuweisende Anforderungen .....  | 26 |
| Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" .....           | 27 |

### **5.3 Referenzierte Dokumente**

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| <b>[Quelle]</b>      | <b>Herausgeber: Titel, Version</b>   |
|----------------------|--|
| [CC]                 | Internationaler Standard: Common Criteria for Information Technology Security Evaluation<br><a href="https://www.commoncriteriaportal.org/cc/">https://www.commoncriteriaportal.org/cc/</a>  |
| [gemRL_PruefSichEig] | gematik: Richtlinie zur Prüfung der Sicherheitseignung   |
| [eIDAS]              | Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG |