

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

gematik Root-CA

Produkttyp Version: 1.5.4-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 558260
Stand: 24.01.2023
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_gematik_Root_CA_PTV_1.5.4-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

| Produkttypversion | Beschreibung der Änderung | Referenz |
|-------------------|---------------------------------------|---------------------------------------------|
| 1.0.0 | Initiale Version auf Dokumentenebene | [gemProdT_gematik_Root_CA_PTV1.0.0] |
| 1.1.0 | Losübergreifende Synchronisation | [gemProdT_gematik_Root_CA_PTV1.1.0] |
| 1.2.0 | P11-Änderungsliste | [gemProdT_gematik_Root_CA_PTV1.2.0] |
| 1.3.0 | P12-Änderungsliste | [gemProdT_gematik_Root_CA_PTV1.3.0] |
| 1.3.1 | Änderungen aus Errata 1.4.3 eingefügt | [gemProdT_gematik_Root_CA_PTV1.3.1] |
| 1.3.1-1 | Anpassung auf Releasestand 1.6.3 | [gemProdT_X.509_gematik_Root_CA_PTV1.3.1-1] |
| 1.4.0-0 | Anpassung auf Releasestand 1.6.4 | [gemProdT_X.509_gematik_Root_CA_PTV1.4.0-0] |
| 1.4.0-1 | Errata 1.6.4-2 | [gemProdT_X.509_gematik_Root_CA_PTV1.4.0-1] |
| 1.4.1-0 | Anpassung auf Releasestand 2.1.2 | [gemProdT_X.509_gematik_Root_CA_PTV1.4.1-0] |
| 1.4.1-1 | Anpassung auf Releasestand 2.1.3 | [gemProdT_X.509_gematik_Root_CA_PTV1.4.1-1] |
| 1.5.0-0 | Anpassung auf Releasestand 3.1.0 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.0-0] |
| 1.5.1-0 | Anpassung auf Releasestand 3.1.2 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.1-0] |
| 1.5.1-1 | Anpassung auf Releasestand 4.0.0 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.1-1] |

| | | |
|---------|------------------------------------------------------|---------------------------------------------|
| 1.5.2-0 | Anpassung zur TI-Baseline 2022-1 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.2-0] |
| 1.5.3-0 | Anpassung auf Releasestand CI_Maintenance_22.2 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.3-0] |
| 1.5.4-0 | Anpassung auf Releasestand CI_Maintenance_22.5 | [gemProdT_X.509_gematik_Root_CA_PTV1.5.4-0] |

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 | 24.01.23 | | freigegeben | gematik |

Inhaltsverzeichnis

| | |
|----------------------------------------------------------------------------------|-----------|
| 1 Einführung | 5 |
| 1.1 Zielsetzung und Einordnung des Dokumentes | 5 |
| 1.2 Zielgruppe | 5 |
| 1.3 Geltungsbereich | 5 |
| 1.4 Abgrenzung des Dokumentes | 5 |
| 1.5 Methodik | 6 |
| 2 Dokumente | 7 |
| 3 Normative Festlegungen | 9 |
| 3.1 Festlegungen zur funktionalen Eignung..... | 9 |
| 3.1.1 Produkttest/Produktübergreifender Test | 9 |
| 3.1.2 Herstellererklärung funktionale Eignung | 13 |
| 3.2 Festlegungen zur sicherheitstechnischen Eignung | 22 |
| 3.2.1 CC-Evaluierung | 22 |
| 3.2.2 Sicherheitsgutachten | 22 |
| 3.2.3 Herstellererklärung sicherheitstechnische Eignung..... | 27 |
| 3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung | 28 |
| 4 Produktypspezifische Merkmale | 30 |
| 5 Anhang A – Verzeichnisse | 31 |
| 5.1 Abkürzungen | 31 |
| 5.2 Tabellenverzeichnis | 31 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps gematik Root-CA oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen 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 normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die normativen Festlegungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an gematik Root-CA-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 normative Festlegungen, 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 dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten normativen Festlegungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativen Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativen Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|---------------------|----------------------------------------------------------------------------------------------------|----------|
| gemSpec_Perf | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform | 2.1924.0 |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.4.0 |
| gemSpec_Net | Übergreifende Spezifikation Netzwerk | 1.22.0 |
| gemSpec_OID | Spezifikation Festlegung von OIDs | 3.12.03 |
| gemKPT_Test | Testkonzept der TI | 2.8.5 |
| gemRL_TSL_SP_CP | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL | 2.10.12 |
| gemSpec_OM | Übergreifende Spezifikation Operations und Maintenance | 1.14.01 |
| gemSpec_X_509_TSP | Spezifikation Trust Service Provider X.509 | 1.19.01 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.124.01 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.224.0 |

Die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte sind informative Beistellungen und sind nicht Gegenstand der Bestätigung / Zulassung.

Tabelle 2: Informative Dokumente und Web-Inhalte

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

Hinweis:

- Ist kein Herausgeber angegeben, wird angenommen, dass die gematik für Herausgabe und Veröffentlichung der Quelle verantwortlich ist.
- Ist keine Version angegeben, bezieht sich die Quellenangabe auf die aktuellste Version.
- Bei Quellen aus gitHub werden als Version Branch und / oder Tag verwendet.

3 Normative Festlegungen

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

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|----------------------------------------------------------------------------------------------------------|-------------------|
| GS-A_4178 | Standardkonforme Namensvergabe in Zertifikaten | gemRL_TSL_SP_CP |
| GS-A_4208 | Ausgabe von Zertifikaten | 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_4348 | Verbot der Erneuerung von Zertifikaten | gemRL_TSL_SP_CP |
| GS-A_4350 | Maximale Gültigkeitsdauer des Zertifikats der gematik Root-CA | gemRL_TSL_SP_CP |
| GS-A_4351 | Maximale Gültigkeitsdauer des Zertifikats eines TSP-X.509 nonQES bei Erzeugung durch die gematik Root-CA | 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 |
| GS-A_5131 | Hash-Algorithmus bei OCSP/CertID | gemSpec_Krypt |
| GS-A_4444 | OID-Festlegung für Certificate Policies | gemSpec_OID |
| 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_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 ServiceTypeIdentifier "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_4588 | CA-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_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 |
| 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_4695 | Zentrale Root-CA für Test- und Referenzumgebung | gemSpec_PKI |
| GS-A_4696 | OCSP-Responder für gematik TeRe-Root-CA im Internet | 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_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_4725 | Eindeutiger SubjectDN durch serialNumber | gemSpec_PKI |
| GS-A_4736 | Umsetzung Zentrale nonQES-Root-CA-Zertifikat | gemSpec_PKI |
| GS-A_4749-01 | TUC_PKI_007: Prüfung Zertifikatstyp | gemSpec_PKI |
| GS-A_4751 | Fehlercodes bei TSL- und Zertifikatsprüfung | gemSpec_PKI |
| GS-A_4829 | TUCs, Fehlerbehandlung | gemSpec_PKI |
| GS-A_4898 | TSL-Grace-Period einer TSL | gemSpec_PKI |
| GS-A_4899 | TSL Update-Prüfintervall | gemSpec_PKI |
| GS-A_4957-01 | Beschränkungen OCSP-Request | gemSpec_PKI |

| | | |
|--------------|-------------------------------------------------------------------|-------------------|
| GS-A_5050 | gematik-Root-CA Statusprüfdienst im Internet | 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_5513 | Wahl des Signaturalgorithmus für Zertifikate | gemSpec_PKI |
| GS-A_5517 | Schlüsselgenerationen der OCSP-Signer-Zertifikate | gemSpec_PKI |
| GS-A_4145 | Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen | gemSpec_Perf |
| GS-A_4146-01 | Performance – Performance-Daten erfassen | gemSpec_Perf |
| GS-A_4147-02 | Performance – Störungssampel – Performance-Daten | gemSpec_Perf |
| GS-A_4148-01 | Performance – Störungssampel – Ereignisnachricht bei Ausfall | gemSpec_Perf |
| GS-A_4149-01 | Performance – Reporting-Daten in Performance-Report | gemSpec_Perf |
| GS-A_5550 | Performance – OCSP Responder – Grundlast | gemSpec_Perf |
| TIP1-A_4015 | Maximale Gültigkeitsdauer des TSL-Signer-CA-Zertifikats | gemSpec_X.509_TSP |
| TIP1-A_4253 | Signierung des Sub-CA-Zertifikats für Produktivumgebung | gemSpec_X.509_TSP |
| TIP1-A_4254 | Signierung des Sub-CA-Zertifikats für Testumgebung | gemSpec_X.509_TSP |
| TIP1-A_5164 | Statusinformation erstellter X.509-Sub-CA-Zertifikate | gemSpec_X.509_TSP |
| TIP1-A_5165 | Statusinformation gesperrter X.509-Sub-CA-Zertifikate | gemSpec_X.509_TSP |
| TIP1-A_5167 | Crosszertifizierung gematik Root-CA-Zertifikate | gemSpec_X.509_TSP |

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen 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 4: Festlegungen zur funktionalen Eignung "Herstellererklärung"

| ID | 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_4191 | Keine Echtdaten in RU und TU | gemKPT_Test |
| TIP1-A_6079 | Updates von Referenzobjekten | gemKPT_Test |
| TIP1-A_6080 | Softwarestand von Referenzobjekten | gemKPT_Test |
| TIP1-A_6081 | Bereitstellung der Referenzobjekte | gemKPT_Test |
| TIP1-A_6085 | Referenzobjekte eines Produkts | gemKPT_Test |
| TIP1-A_6088 | Unterstützung bei Fehlernachstellung | gemKPT_Test |
| TIP1-A_6093 | Ausprägung der Referenzobjekte | gemKPT_Test |
| TIP1-A_6517-01 | Eigenverantwortlicher Test: TBI | gemKPT_Test |
| TIP1-A_6518 | Eigenverantwortlicher Test: TDI | gemKPT_Test |
| 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 |
| 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 |
| 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_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_4189 | Prüfungspflicht für Person, Schlüsselpaar, Schlüsselaktivierungsdaten und Name | 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_4194 | Identifikation des Antragstellers und Dokumentation bei der Beantragung eines CA-Zertifikats | 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_4204 | Bearbeitung von Zertifikatsanträgen eines TSP-X.509 nonQES durch die gematik Root-CA | gemRL_TSL_SP_CP |
| GS-A_4206 | Prüfung auf Korrektheit des Schlüsselpaars eines TSP-X.509 nonQES | 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_4215 | Bedingungen für eine Zertifizierung nach Schlüsselerneuerung | gemRL_TSL_SP_CP |
| GS-A_4221 | Anzeige der Kompromittierung des privaten Signaturschlüssels | gemRL_TSL_SP_CP |
| GS-A_4222 | Beschreibung der Bedingungen für die Sperrung des Zertifikats eines TSP-X.509 nonQES | gemRL_TSL_SP_CP |
| GS-A_4223 | Obligatorische Gründe für die Sperrung des Zertifikats eines TSP-X.509 nonQES durch die gematik Root-CA | 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_4232 | Informationspflicht der gematik Root-CA bei Sperrung der Zertifikats eines TSP-X.509 nonQES | gemRL_TSL_SP_CP |
| GS-A_4242 | Dokumentationspflicht für Prozesse der Schlüssel hinterlegung | gemRL_TSL_SP_CP |
| GS-A_4245 | Anzeige von Änderung an der Gesellschafterstruktur des Betreibers | gemRL_TSL_SP_CP |

| | | |
|-----------|-----------------------------------------------------------------------------|-----------------|
| GS-A_4246 | Bereitstellung aktueller Liste registrierter TSP | 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_4280 | Fristen bei Einstellung des Zertifizierungsbetriebs für die gematik Root-CA | gemRL_TSL_SP_CP |
| GS-A_4282 | Erforderliche Form bei Einstellung des Zertifizierungsbetriebs | gemRL_TSL_SP_CP |
| 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 Schlüsselpaars | 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 Schlüsselpaars | 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_4355 | Maximale Gültigkeitsdauer des Zertifikats eines TSP-X.509 nonQES bei Erzeugung durch den 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_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 |

| | | |
|-----------|--------------------------------------------------------------------------------------------------------------------------|-----------------|
| 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_4933 | CP-Test, Zertifikatsprofile für Testzertifikate | gemRL_TSL_SP_CP |
| GS-A_5075 | Schlüsselbackup bei der gematik | 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 |
| GS-A_5123 | Verfahrensbeschreibung Datensicherung der gematik Root-CA | gemRL_TSL_SP_CP |
| GS-A_5468 | Planmäßige Schlüsselerneuerung der gematik Root-CA | gemRL_TSL_SP_CP |
| GS-A_5469 | Verwendung des neuesten Schlüssels der gematik Root-CA | gemRL_TSL_SP_CP |
| A_15590 | Zertifikatslaufzeit bei Erstellung von X.509-Zertifikaten mit RSA 2048 Bit | 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_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 |
| GS-A_4257 | Hauptsitz und Betriebsstätte | 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_4727 | PKI-Separierung von Test- und Produktivumgebung in der TI | gemSpec_PKI |
| GS-A_4732 | Extension der CA-Zertifikate | gemSpec_PKI |
| GS-A_5050 | gematik-Root-CA Statusprüfdienst im Internet | gemSpec_PKI |
| GS-A_5052 | gematik Root-CA Zertifikatsstatus | 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_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_4149-01 | Performance – Reporting-Daten in Performance-Report | gemSpec_Perf |
| GS-A_4155 | Performance – zentrale Dienste – Verfügbarkeit | gemSpec_Perf |

| | | |
|-------------|------------------------------------------------------------------------------------------------------------|-------------------|
| GS-A_4159 | Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast | gemSpec_Perf |
| 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_3562 | Schnittstellen gematik-Root-CA | gemSpec_X.509_TSP |
| TIP1-A_3655 | Certificate Policy des gematik-Root-CA | gemSpec_X.509_TSP |
| TIP1-A_3656 | abgestimmtes Antrags- und Sperrverfahren | gemSpec_X.509_TSP |
| TIP1-A_3657 | Gesicherte Zertifikatserstellung der X-509-Sub-CA-Zertifikate | gemSpec_X.509_TSP |
| TIP1-A_3658 | Antragsdaten X.509-Sub-CA-Zertifikat | gemSpec_X.509_TSP |
| TIP1-A_3662 | Registrierung einer Test-TSP-X.509-CA | gemSpec_X.509_TSP |
| TIP1-A_3663 | Dokumentation von Sperrungen | 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_3879 | Ausstellung von X.509-Zertifikate für zugelassene TSP-X.509 | gemSpec_X.509_TSP |
| TIP1-A_3880 | Bestätigung Auflagen bei Widerruf der Zulassung | gemSpec_X.509_TSP |
| TIP1-A_4250 | Betriebskonzept gematik-Root-CA | gemSpec_X.509_TSP |
| TIP1-A_4251 | Auditierverfahren gematik-Root-CA | gemSpec_X.509_TSP |
| TIP1-A_4252 | Antragsverfahren Sub-CA-Zertifikate | gemSpec_X.509_TSP |
| TIP1-A_4255 | Ausgabe des Sub-CA-Zertifikats | gemSpec_X.509_TSP |
| TIP1-A_4427 | Betrieb einer Test-TSP-X.509 | gemSpec_X.509_TSP |
| TIP1-A_4428 | Registrierung eines Test-TSP-X.509 | gemSpec_X.509_TSP |
| TIP1-A_4434 | Verfahren zur Zeitsynchronisierung gematik-Root-CA | gemSpec_X.509_TSP |
| TIP1-A_5166 | Rückmeldung Sperrungen | gemSpec_X.509_TSP |
| TIP1-A_5168 | Bereitstellung gematik Root-CA- und Sub-Ca-Zertifikate und Fingerprints im Internet | gemSpec_X.509_TSP |

| | | |
|-------------|---------------------------------------------------------------------------|-------------------|
| TIP1-A_5376 | Erreichbarkeit des Sperrdienstes von TSP-X.509 nonQES und gematik Root-CA | gemSpec_X.509_TSP |
|-------------|---------------------------------------------------------------------------|-------------------|

3.2 Festlegungen 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 Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig_DS]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

| ID | 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 |
| 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 |
| 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_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 |
| 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_17124-01 | 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_4357-01 | 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_4367 | Zufallszahlengenerator | gemSpec_Krypt |
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
| GS-A_4384-01 | 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_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_5518 | Prüfung Kurvenpunkte bei einer Zertifikatserstellung | gemSpec_Krypt |
| A_20574-01 | Beachtung der ISI-LANA für Übergänge zu Fremdnetzen | gemSpec_Net |
| GS-A_4062-01 | Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen | 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_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |
| TIP1-A_3555 | Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA | gemSpec_X.509_TSP |
| TIP1-A_3660 | Trennung der TSP-X.509-Betriebsumgebungen | gemSpec_X.509_TSP |
| TIP1-A_3664 | Sperrinformationen | gemSpec_X.509_TSP |
| TIP1-A_3881 | Schutzbedarf darf nicht verringert werden | gemSpec_X.509_TSP |
| TIP1-A_4015 | Maximale Gültigkeitsdauer des TSL-Signer-CA-Zertifikats | 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_4233 | Löschung von gematik-Root-CA Zertifikats- und Sperraufträge | gemSpec_X.509_TSP |
| TIP1-A_4235 | Fehlerprotokollierung | gemSpec_X.509_TSP |
| TIP1-A_5371 | Systemtechnische Trennung bei Aufbau und Betrieb der gematik Root-CA | gemSpec_X.509_TSP |
| A_17124 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| GS-A_4384 | TLS-Verbindungen | gemSpec_Krypt |

3.2.3 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Festlegungen 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: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---------------------------------------------------------------------------------------------------|---------------------|
| GS-A_2355-02 | 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_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_5559-01 | 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_5624-01 | Auditrechte der gematik zur Informationssicherheit | gemSpec_DS_Anbieter |
| A_15590 | Zertifikatslaufzeit bei Erstellung von X.509-Zertifikaten mit RSA 2048 Bit | 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_5541 | TLS-Verbindungen als TLS-Klient zur Störungssampel 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 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

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

Tabelle 7: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

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

4 Produktypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produktyps vor.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

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

5.2 Tabellenverzeichnis

| | |
|-------------------------------------------------------------------------------------------------|----|
| Tabelle 1: Dokumente mit normativen Festlegungen | 7 |
| Tabelle 2: Informative Dokumente und Web-Inhalte | 7 |
| Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" | 9 |
| Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellererklärung" | 14 |
| Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" | 22 |
| Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung" | 27 |
| Tabelle 7: Festlegungen zur elektrischen, mechanischen und physikalischen Eignung | 29 |