

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Trust Service Provider X.509 QES

Produkttyp Version: 1.9.6-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 536306
Stand: 07.12.2022
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_X509_TSP_QES_PTV_1.9.6-0

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_X.509_TSP_QES_PTV1.0.0]
1.1.0	Losübergreifende Synchronisation	[gemProdT_X.509_TSP_QES_PTV1.1.0]
1.2.0	P11-Änderungsliste	[gemProdT_X.509_TSP_QES_PTV1.2.0]
1.3.0	P12-Änderungsliste	[gemProdT_X.509_TSP_QES_PTV1.3.0]
1.5.0	Änderungen aus Errata 1.4.3 und 1.4.6 eingefügt	[gemProdT_X.509_TSP_QES_PTV1.5.0]
1.6.0	Anpassung OPB1	[gemProdT_X.509_TSP_QES_PTV1.6.0]
1.6.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_X.509_TSP_QES_PTV1.6.0-1]
1.7.0-0	Anpassung auf Releasestand 1.6.4	[gemProdT_X.509_TSP_QES_PTV1.7.0-0]
1.7.1-0	Errata 1.6.4-1	[gemProdT_X.509_TSP_QES_PTV1.7.1-0]
1.7.2-0	Errata 1.6.4-3	[gemProdT_X.509_TSP_QES_PTV1.7.2-0]
1.8.0-0	Anpassung auf Releasestand 2.1.1	[gemProdT_X.509_TSP_QES_PTV1.8.0-0]
1.8.1-0	Anpassung an Releasestand 2.1.2	[gemProdT_X.509_TSP_QES_PTV1.8.1-0]
1.8.2-0	Anpassung an Releasestand 2.1.3	[gemProdT_X.509_TSP_QES_PTV1.8.2-0]

1.9.0-0	Anpassung an Releasestand 3.1.0	[gemProdT_X.509_TSP_QES_PTV1.9.0-0]
1.9.0-1	Anpassung an Releasestand 3.1.1	[gemProdT_X.509_TSP_QES_PTV1.9.0-1]
1.9.1-0	Anpassung an Releasestand 3.1.2	[gemProdT_X.509_TSP_QES_PTV1.9.1-0]
1.9.2-0	Anpassung an Releasestand 3.1.3	[gemProdT_X.509_TSP_QES_PTV1.9.2-0]
1.9.2-1	Anpassung an Releasestand 3.1.3 Hotfix 2	[gemProdT_X.509_TSP_QES_PTV1.9.2-1]
1.9.3-0	Anpassung an Releasestand 4.0.0	[gemProdT_X.509_TSP_QES_PTV1.9.3-0]
1.9.4-0	Anpassung zur TI-Baseline 2022-1, redaktionelle Anpassungen in Kap. 4.1	[gemProdT_X.509_TSP_QES_PTV1.9.4-0]
1.9.5-0	Anpassung auf Releasestand CI_Maintenance_22.4	[gemProdT_X.509_TSP_QES_PTV1.9.5-0]
1.9.6-0	Anpassung auf Releasestand CI_Maintenance_22.5	[gemProdT_X.509_TSP_QES_PTV1.9.6-0]

Historie Produkttypsteckbrief

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

Version	Datum	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	07.12.22		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	15
3.2 Festlegungen zur sicherheitstechnischen Eignung	21
3.2.1 CC-Evaluierung	21
3.2.2 Sicherheitsgutachten	21
3.2.3 Sicherheitsbestätigung.....	23
3.2.4 Herstellererklärung sicherheitstechnische Eignung.....	23
3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung	26
4 Produkttypspezifische Merkmale	27
4.1 Optionale Ausprägungen	27
5 Anhang A – Verzeichnisse	28
5.1 Abkürzungen	28
5.2 Tabellenverzeichnis	28

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 Trust Service Provider X.509 QES 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 Trust Service Provider X.509 QES-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

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.14.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.10.2
gemSpec_X_509_TSP	Spezifikation Trust Service Provider X.509	1.19.1
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.24.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.14.0
gemSpec_ServiceMon	Spezifikation Service Monitoring	1.5.0
gemSpec_OID	Spezifikation Festlegung von OIDs	3.12.3
gemKPT_Test	Testkonzept der TI	2.8.5
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.4.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.22.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.24.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte als ganzes normativ und gelten mit.

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[CP-HPC]	Bundesärztekammer et al: Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.0)	1.0.0

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

Tabelle 3 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	
[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	

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 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

ID	Bezeichnung	Quelle (Referenz)
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
GS-A_4384-01	TLS-Verbindungen	gemSpec_Krypt
GS-A_3832	DNS-Protokoll, Resolver-Implementierungen	gemSpec_Net
GS-A_3834	DNS-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS-A_3842-01	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_4442-02	OID-Festlegung Rolle für Berufsgruppen	gemSpec_OID
GS-A_4444	OID-Festlegung für Certificate Policies	gemSpec_OID
GS-A_4445-06	OID-Festlegung für Zertifikatstypen	gemSpec_OID
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 Störungssampel	gemSpec_OM
A_15676	Reihenfolge der Elemente im SubjectDN von X.509-Zertifikaten	gemSpec_PKI
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
A_17689	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
A_17700	TSL-Auswertung 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
A_19500	Statusprüfdienst – Hinterlegung OCSP-Signer-Zertifikat	gemSpec_PKI
GS-A_4588	CA-Namen für Test-PKI der TI	gemSpec_PKI
GS-A_4589	EE-Namen für Test-PKI der TI	gemSpec_PKI
GS-A_4590	Zertifikatsprofile für Test-PKI	gemSpec_PKI
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI

GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_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_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_4698	Pseudo-QES PKI für PKI-TeRe	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_4717-02	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_4724	Komplettspernung aller Zertifikate einer Karte	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_4948	Umsetzung QES-CA-Zertifikate	gemSpec_PKI
GS-A_4957-01	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_5042	Kodierung der X.509-Zertifikate für HBA und SMC-B	gemSpec_PKI

GS-A_5043	Auflösung von OCSP-Adressen 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_5124-01	OCSP-Responses mit Parameter Nonce gemäß [RFC6960]	gemSpec_PKI
GS-A_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	gemSpec_PKI
GS-A_5513	Wahl des Signaturalgorithmus für Zertifikate	gemSpec_PKI
GS-A_5533-01	Umsetzung Zertifikatsprofil C.HP.QES	gemSpec_PKI
A_21975	Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21976	Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21980	Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
A_21981-02	Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02)	gemSpec_Perf
A_21982-01	Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_22000	Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02)	gemSpec_Perf
A_22001-01	Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02)	gemSpec_Perf
A_22002	Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22004	Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)	gemSpec_Perf
A_22047	Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_22429	Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02)	gemSpec_Perf
A_22482	Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02)	gemSpec_Perf

A_22489	Performance - Rohdaten - Spezifika TSP X.509 - Duration (Rohdatenerfassung v.02)	gemSpec_Perf
A_22490	Performance - Rohdaten - Spezifika TSP X.509 - Operation (Rohdatenerfassung v.02)	gemSpec_Perf
A_22491	Performance - Rohdaten - Spezifika TSP X.509 - Status (Rohdatenerfassung v.02)	gemSpec_Perf
A_22492	Performance - Rohdaten - Spezifika TSP X.509 - Message (Rohdatenerfassung v.02)	gemSpec_Perf
A_22500-01	Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_22513-01	Performance - Rohdaten - Message-Block im Fehlerfall (Rohdatenerfassung v.02)	gemSpec_Perf
GS-A_4145	Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen	gemSpec_Perf
GS-A_5550	Performance – OCSP Responder – Grundlast	gemSpec_Perf
A_15166	Nutzer der Schnittstelle I_Monitoring_Update, Zertifikatsprüfung	gemSpec_ServiceMon
TIP1-A_7117	Service Monitoring und Client, I_Monitoring_Update, Webservice	gemSpec_ServiceMon
TIP1-A_7120	Service Monitoring und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittlung	gemSpec_ServiceMon
TIP1-A_7126	Nutzer des Service Monitorings I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung	gemSpec_ServiceMon
TIP1-A_7128	Nutzer des Service Monitorings I_Monitoring_Update, maximale HTTP-Nachrichtenlänge	gemSpec_ServiceMon
TIP1-A_3586	professionItem und der professionOID für LE (QES)	gemSpec_X.509_TSP
TIP1-A_3594	Bereitstellungszeitpunkt der Zertifikatsstatusinformation für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3886	OCSP-Adresse im X.509-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 5: 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_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1-A_4191	Keine Echtdateien in RU und TU	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6085	Referenzobjekte eines Produkts	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6517-01	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_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_4911	CP-Test, Standardkonforme Namensvergabe in Testzertifikaten	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
GS-A_4915	CP-Test, Kein Bezug zu Echtdaten von Personen oder Organisationen	gemRL_TSL_SP_CP
GS-A_4916	CP-Test, Kennzeichnung von personen- bzw. organisationsbezogenen Testzertifikaten	gemRL_TSL_SP_CP
GS-A_4919	CP-Test, Testkennzeichen in 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_4931	CP-Test, Maximale Gültigkeitsdauer von Testzertifikaten	gemRL_TSL_SP_CP
GS-A_4933	CP-Test, Zertifikatsprofile für Testzertifikate	gemRL_TSL_SP_CP
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_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_3824	FQDN von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform	gemSpec_Net
GS-A_3931	DNSSEC-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4010	Standards für IPv6	gemSpec_Net
GS-A_4011	Unterstützung des Dual-Stack Mode	gemSpec_Net
GS-A_4012	Leistungsanforderungen an den Dual-Stack Mode	gemSpec_Net
GS-A_4013	Nutzung von UDP/TCP-Portbereichen	gemSpec_Net
GS-A_4018	Dokumentation UDP/TCP-Portbereiche Anbieter	gemSpec_Net
GS-A_4024-01	Nutzung IP-Adressbereiche	gemSpec_Net
GS-A_4027	Reporting IP-Adressbereiche	gemSpec_Net
GS-A_4033	Statisches Routing TI-Übergabepunkte	gemSpec_Net

GS-A_4759-01	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_3702	Inhalt der Selbstauskunft von Produkten außer Karten	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_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	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_4584	Verwendung von Berufsgruppenkennzeichen	gemSpec_PKI
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
GS-A_4687	Statusprüfdienst – Response Status sigRequired	gemSpec_PKI
GS-A_4689	Statusprüfdienst – Zeitquelle von producedAt	gemSpec_PKI
GS-A_4694	Betrieb von OCSP-Responder für Test-PKI-CAs	gemSpec_PKI
GS-A_4704	Nutzung von CA mit spezifischem Verwendungszweck	gemSpec_PKI
GS-A_4713	Zeichensatz für den Fortsatz der Telematik-ID	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
GS-A_4731	Attribute der CA-Zertifikate	gemSpec_PKI
GS-A_4735	Namenskonvention für CA-Zertifikate	gemSpec_PKI
GS-A_4901	Einheitliche Admission in Zertifikaten einer Karte	gemSpec_PKI
GS-A_5337	Größenbeschränkung von X.509 Zertifikaten auf Karten	gemSpec_PKI
GS-A_5483	Aufnahme der Pseudo-QES CA in die Pseudo-BNetzA-VL	gemSpec_PKI
GS-A_5512	Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 QES	gemSpec_PKI
GS-A_5529	Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 QES	gemSpec_PKI
A_21978	Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21979	Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22005	Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
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
A_18040	Verpflichtung Meldung Übersetzung QES Internet-OCSP- in TI-OCSP-Adressen für TSL	gemSpec_X.509_TSP
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_3560	Obligatorische Schnittstellen TSP-X.509 QES	gemSpec_X.509_TSP
TIP1-A_3585	Eingangsdaten Leistungserbringerzertifikat (QES)	gemSpec_X.509_TSP
TIP1-A_3588	Abstimmung des Antragsverfahrens	gemSpec_X.509_TSP
TIP1-A_3591	Eindeutigkeit von X.509-Personen- und Organisationszertifikaten	gemSpec_X.509_TSP
TIP1-A_3592	Erstellung von X.509-Personen- und Organisationszertifikaten	gemSpec_X.509_TSP
TIP1-A_3596	Umsetzung Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES für Personen- und Organisationszertifikate	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
TIP1-A_3885	Umgang mit nicht-sicherheitskritischen Incidents für QES-Zertifikate	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_3888	Zertifikatsstatusinformationen der Personen- und Organisationszertifikate	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_5088	Sektorzulassung für zugelassene TSP-X.509	gemSpec_X.509_TSP
TIP1-A_5092	Negative Prüfung von QES-Zertifikatsanträgen	gemSpec_X.509_TSP
TIP1-A_5094	Rückmeldung Zertifikatsinformationen (QES) an Bestätigende Stelle	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 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
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

GS-A_4358	X.509-Identitäten für die Erstellung und Prüfung 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_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_4817	Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI	gemSpec_Net
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_3595	Anforderungen von LEO- und KTR-Institutionen	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_5087	Berücksichtigung und Umsetzung übergeordneter Herausgeberpolicies	gemSpec_X.509_TSP

3.2.3 Sicherheitsbestätigung

Der Produkttyp erfordert eine Bestätigung des Status als qualifizierter Vertrauensdiensteanbieter nach Art. 3 Nr. 20 der eIDAS-Verordnung [eIDAS]. Diese Bestätigung dient als Sicherheitsbestätigung und erfolgt durch die Vorlage des von der Bundesnetzagentur ausgestellten Qualifikationsbescheids bei der gematik. Der Nachweis der im Folgenden ggf. aufgeführten Festlegungen erfolgt implizit durch den Qualifikationsbescheid.

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsbestätigung"

ID	Bezeichnung	Quelle (Referenz)
GS-A_3834	DNS-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS-A_3932	Abfrage der in der Topologie am nächsten stehenden Nameservers	gemSpec_Net
GS-A_4672-01	Statusprüfdienst QES gemäß den Vorgaben von eIDAS und Standards	gemSpec_PKI
TIP1-A_3583	Erstellung QES-Zertifikat nach eIDAS	gemSpec_X.509_TSP
TIP1-A_3584	Prozessgestaltung für QES-Zertifikat	gemSpec_X.509_TSP
TIP1-A_3589	Umsetzung Registrierungsdienst TSP-X.509 QES	gemSpec_X.509_TSP
TIP1-A_3590	Eindeutige Verbindung Personen- und Organisationszertifikatsnehmer und privater Schlüssel	gemSpec_X.509_TSP
TIP1-A_3596	Umsetzung Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3641	Sperrdienst gemäß den Vorgaben von eIDAS	gemSpec_X.509_TSP
TIP1-A_4243	Prüfung der Berechtigung des Antragstellers für QES-Zertifikate	gemSpec_X.509_TSP

3.2.4 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 8: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
----	-------------	-------------------

GS-A_2355-02	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_4468-02	kDSM: Jährlicher Datenschutzbericht der TI	gemSpec_DS_Anbieter
GS-A_4473-01	kDSM: Unverzögliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_4478-01	kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes	gemSpec_DS_Anbieter
GS-A_4479-01	kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter
GS-A_5555	Unverzögliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzögliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5559-01	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_5564	kDSM: Ansprechpartner für Datenschutz	gemSpec_DS_Anbieter
GS-A_5565	kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS-A_5566	kDSM: Sicherstellung der Datenschutzerfordernungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS-A_5624-01	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_5625	kDSM: Auditrechte der gematik zum Datenschutz	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_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	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 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
TIP1-A_5093	Eingangsdaten der Bestätigungsprüfende Stelle für Produktion von QES-Zertifikaten für Leistungserbringer	gemSpec_X.509_TSP

3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

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

4 Produktypspezifische Merkmale

4.1 Optionale Ausprägungen

Die bisherige Wahlfreiheit, ob Produkt Performance-Rohdaten oder Performance-Reports an die gematik übermittelt werden besteht nicht mehr. Die Lieferung von Performance-Rohdaten ist verbindlich vorgeschrieben.

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: Mitgeltende Dokumente und Web-Inhalte	7
Tabelle 3 Informative Dokumente und Web-Inhalte	8
Tabelle 4: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"	9
Tabelle 5: Festlegungen zur funktionalen Eignung "Herstellererklärung"	15
Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"	21
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsbestätigung"	23
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"	23