Einführung der Gesundheitskarte

Produkttypsteckbrief

Prüfvorschrift

Trust Service Provider X.509 nonQES - HBA

Produkttypversion: **1.7.1-1**

Produkttypstatus: **freigegeben**

Version:	1.0.0
Revision:	\main\rel_opb1\rel_ors2\3
Stand:	18.12.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenz:	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.7.1-1]

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_HBA_PTV1.0.0]
1.1.0	Losübergreifende Synchronisation	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.1.0]
1.2.0	P11-Änderungsliste	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.2.0]
1.3.0	P12-Änderungsliste	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.3.0]
1.5.0	Änderungen durch Errata 1.4.3 und 1.4.6 eingefügt	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.5.0]
1.6.0	Anpassung OPB1, Kapitel 3.2.2 ergänzt	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.6.0]
1.6.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.6.0-1]
1.7.0-0	Anpassung auf Releasestand 1.6.4	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.7.0-0]
1.7.0-1	Errata 1.6.4-2	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.7.0-1]
1.7.1-0	Errata 1.6.4-3	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.7.1-0]
1.7.1-1	Anpassung auf Releasestand 2.1.1	[gemProdT_X.509_TSP_nonQES_HBA_PTV1.7.1-1]

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	18.12.17		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

Nach Inkrafttreten der eIDAS-Verordnung wurde die Anforderungslage der gematik entsprechend angepasst. Signaturgesetz (SigG) und -verordnung (SigV) sind weiterhin gültig und finden dort Anwendung, wo sie der eIDAS-Verordnung nicht widersprechen. SigG und SigV sollen zukünftig durch das deutsche Vertrauensdienstegesetz (VDG) abgelöst werden. Mit Verabschiedung des Vertrauensdienstegesetzes kann es in diesem Dokument daher zu Anpassungen und Konkretisierungen entsprechend der geänderten Rechtslage kommen.

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 - HBA in der Produkttypversion 1.7.1-1 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[1] durch die gematik.

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 - HBA-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] 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.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

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

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

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

Afo-ID: Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

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

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumentenkürzel	Bezeichnung des Dokuments	Version
gemKPT_Test	Testkonzept	1.10.0
gemRL_TSL_SP_CP	Certificate Policy	2.1.0
gemSpec_DSM	Spezifikation koordinierendes DSM	1.3.1
gemSpec_ISM	Spezifikation koordinierendes ISM	1.4.1
gemSpec_Krypt	Spezifikation kryptographischer Algorithmen in der TI	2.9.0
gemSpec_Net	Spezifikation Netzwerk	1.12.0
gemSpec_OID	Spezifikation Festlegung von OIDs	3.1.0
gemSpec_OM	Spezifikation Operations und Maintenance	1.8.0
gemSpec_Perf	Spezifikation Performance und Mengengerüst	2.3.0
gemSpec_PKI	Spezifikation PKI (mit Anhang A)	2.1.0
gemSpec_SiBetrUmg	Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung	1.4.0
gemSpec_Sich_DS	Spezifikation Sicherheits-/Datenschutzanforderungen	1.4.1
gemSpec_St_Ampel	Spezifikation Störungsampel	1.5.0
gemSpec_X.509_TSP	Spezifikation Trust Service Provider X.509	1.9.0

Tabelle 2: Mitgeltende Dokumente

Dokumentenkürzel	Bezeichnung des Dokuments
BAEK_HBA_Attr	Bundesärztekammer: Zertifikatsprofile für X.509 Attributzertifikate; Version 2.3.2
BAEK_HBA_Cert	Bundesärztekammer: Zertifikatsprofile für X.509 Basiszertifikate; Version 2.3.2
BZÄK_HBA_Cert	Bundeszahnärztekammer: Zertifikatsprofil des elektronischen Zahnarztausweises; Version 2.2
PTK_HBA_Cert	Bundespsychotherapeutenkammer: Zertifikatsprofile für X.509 Basiszertifikate, Version 1.1
PTK_HBA_Attr	Bundespsychotherapeutenkammer: Zertifikatsprofile für X.509 Attributzertifikate, Version 1.1

Dokumentenkürzel	Bezeichnung des Dokuments
CP-HPC	Bundesärztekammer et al: Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.0)

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 3: 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_4181	Eindeutigkeit der Namensform des Zertifikatsnehmers	gemRL_TSL_SP_CP
GS-A_4213	Zulässige Nutzungsarten	gemRL_TSL_SP_CP
GS-A_4303	Festlegung der Schlüsselverwendung (keyUsage)	gemRL_TSL_SP_CP
GS-A_4352	Maximale Gültigkeitsdauer eines Endbenutzerzertifikats	gemRL_TSL_SP_CP
GS-A_4911	CP-Test, Standardkonforme Namensvergabe in Testzertifikaten	gemRL_TSL_SP_CP
GS-A_4914	CP-Test, Eindeutigkeit der Namensform des Zertifikatsnehmers	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_4929	CP-Test, Funktionsweise des Statusabfragedienst	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
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
GS-A_5131	Hash-Algorithmus bei OCSP / CertID	gemSpec_Krypt
GS-A_5518	Prüfung Kurvenpunkte bei einer Zertifikatserstellung	gemSpec_Krypt
GS-A_4832	Path MTU Discovery	gemSpec_Net
GS-A_4013	Nutzung von UDP/TCP-Portbereichen	gemSpec_Net
GS-A_4024	Nutzung IP-Adressbereiche	gemSpec_Net

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4033	Statisches Routing TI-Übergabepunkte	gemSpec_Net
GS-A_4036	Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS-A_4763	Einsatz von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS-A_4054	Paketfilter Default Deny	gemSpec_Net
GS-A_3932	Abfrage der in der Topologie am nächsten stehenden Nameservers	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_3832	DNS-Protokoll, Resolver-Implementierungen	gemSpec_Net
GS-A_3833	DNSSEC-Protokoll, Resolver-Implementierungen	gemSpec_Net
GS-A_3840	DNS-Resolver, Nutzung von DNSSEC	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_3934	NTP-Client-Implementierungen, Protokoll NTPv4	gemSpec_Net
GS-A_3937	NTP-Client-Implementierungen, Association Mode und Polling Intervall	gemSpec_Net
GS-A_3939	Produkttypen der TI-Plattform, Zeitsynchronisierung nach Neustart	gemSpec_Net
GS-A_3946	NTP-Client-Implementierungen, SNTP	gemSpec_Net
GS-A_4442	OID-Festlegung Rolle für Berufsgruppen	gemSpec_OID
GS-A_4444	OID-Festlegung für Certificate Policies	gemSpec_OID
GS-A_4445	OID-Festlegung für Zertifikatstypen	gemSpec_OID
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	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_3804	Eigenschaften eines FehlerLog-Eintrags	gemSpec_OM
GS-A_3807	Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung	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_4146	Performance - Performance-Daten erfassen	gemSpec_Perf
GS-A_4147	Performance - Störungsampel - Performance-Daten	gemSpec_Perf
GS-A_4148	Performance - Störungsampel - Ereignisnachricht bei Ausfall	gemSpec_Perf
GS-A_4149	Performance - Reporting-Daten in Performance-Report	gemSpec_Perf
GS-A_4145	Performance - zentrale Dienste - Robustheit gegenüber Lastspitzen	gemSpec_Perf

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5550	Performance – OCSP Responder – Grundlast	gemSpec_Perf
~~GS-A_4159~~	~~Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast~~	~~gemSpec_Perf~~
GS-A_4160	Performance - OCSP-Responder - Performance Reporting - Daten nach Zertifikatstyp	gemSpec_Perf
GS-A_5513	Wahl des Signaturalgorithmus für Zertifikate	gemSpec_PKI
GS-A_4697	PKI für Test- und Referenzumgebung	gemSpec_PKI
GS-A_4705	Verarbeitung von Sonderzeichen in PKI-Komponenten	gemSpec_PKI
GS-A_4706	Vorgaben zu SubjectDN von CA- und OCSP-Zertifikaten	gemSpec_PKI
GS-A_4709	Abbildung der Telematik-ID in Admission-Struktur	gemSpec_PKI
GS-A_4714	Kodierung der Attribute in X.509-Zertifikaten	gemSpec_PKI
GS-A_4715	Maximale Stringlänge der Attribute im SubjectDN	gemSpec_PKI
GS-A_4717	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	Komplettsperrung aller Zertifikate einer Karte	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_5042	Kodierung der X.509-Zertifikate für HBA und SMC-B	gemSpec_PKI
GS-A_5531	Umsetzung Zertifikatsprofil C.HP.AUT	gemSpec_PKI
GS-A_5532	Umsetzung Zertifikatsprofil C.HP.ENC	gemSpec_PKI
GS-A_4738	Eindeutige Identifizierung der OCSP-Signer-Zertifikate	gemSpec_PKI
GS-A_4741	Umsetzung Zertifikatsprofil C.GEM.OCSP	gemSpec_PKI
GS-A_4936	Attribute der CRL-Signer-Zertifikate	gemSpec_PKI
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS-A_4829	TUCs, Fehlerbehandlung	gemSpec_PKI
GS-A_5043	Auflösung von OCSP-Adressen im Internet	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_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4652	TUC_PKI_018: Zertifikatsprüfung in der TI	gemSpec_PKI
GS-A_4653	TUC_PKI_002: Gültigkeitsprüfung des Zertifikats	gemSpec_PKI
GS-A_4654	TUC_PKI_003: CA-Zertifikat finden	gemSpec_PKI
GS-A_4655	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	gemSpec_PKI
GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	gemSpec_PKI
GS-A_4657	TUC_PKI_006: OCSP-Abfrage	gemSpec_PKI
GS-A_4660	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS-A_4749	TUC_PKI_007: Prüfung Zertifikatstyp	gemSpec_PKI
GS-A_4661	kritische Erweiterungen in Zertifikaten	gemSpec_PKI
GS-A_4662	Bedingungen für TLS-Handshake	gemSpec_PKI
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	gemSpec_PKI
GS-A_4669	Umsetzung Statusprüfdienst	gemSpec_PKI
GS-A_5053	TI-Zertifikatstypen im Internet	gemSpec_PKI
GS-A_5051	TSP-X.509 nonQES Zertifikatsstatus	gemSpec_PKI
GS-A_4674	OCSP-Requests gemäß [RFC2560] und [Common-PKI]	gemSpec_PKI
GS-A_4957	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_4676	OCSP-Responses gemäß [Common-PKI]	gemSpec_PKI
GS-A_4677	Spezifikationskonforme OCSP-Responses	gemSpec_PKI
GS-A_4678	Signierte OCSP-Responses	gemSpec_PKI
GS-A_5517	Schlüsselgenerationen der OCSP-Signer-Zertifikate	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_5090	Statusprüfdienst - Keine Angabe von Sperrgründen	gemSpec_PKI
GS-A_4693	Statusprüfdienst - Positive Statement	gemSpec_PKI
GS-A_4694	Betrieb von OCSP-Responder für Test-PKI-CAs	gemSpec_PKI
TIP1-A_5993	Störungsampel und Client, I_Monitoring_Update, WebService	gemSpec_St_Ampel
TIP1-A_5996	Störungsampel und Client, I_Monitoring_Update, maximale Zeitabweichung zwischen Berichtszeitraum und Nachrichtenübermittelung	gemSpec_St_Ampel
TIP1-A_5998	Nutzer der Störungsampel I_Monitoring_Update,	gemSpec_St_Ampel

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Zertifikatsprüfung	
TIP1-A_5997	Nutzer der Störungsampel I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung	gemSpec_St_Ampel
TIP1-A_6002	Nutzer der Störungsampel I_Monitoring_Update, Selbstauskunft als Bestandteil jeder SOAP-Nachricht	gemSpec_St_Ampel
TIP1-A_3894	Obligatorisch abzuleitende Sub-CAs unterhalb der gematikRoot-CA	gemSpec_X.509_TSP
TIP1-A_3570	Eingangsdaten Leistungserbringerzertifikat	gemSpec_X.509_TSP
TIP1-A_3571	professionItem und professionOID für LE	gemSpec_X.509_TSP
TIP1-A_3577	Optionale Eingangsdaten	gemSpec_X.509_TSP
TIP1-A_3886	OCSP-Adresse im X.509-Zertifikate	gemSpec_X.509_TSP
TIP1-A_3594	Bereitstellungszeitpunkt der Zertifikatsstatusinformation für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3639	Weitergabe der Zertifikatsstatusinformationen von Personen- und Organisationszertifikaten an den OCSP-Responder	gemSpec_X.509_TSP
TIP1-A_3640	Information an den Sperrantragsteller für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP

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 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6516	Eigenverantwortlicher Test: Test & Transitionmanager	gemKPT_Test
TIP1-A_6517	Eigenverantwortlicher Test: TBV	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_2769	Kompatibilität und Interoperabilität der Schnittstellen	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_2781	Dauerhafte Verfügbarkeit in der Testumgebung	gemKPT_Test
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6525	Produkttypen: Testziele	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6531	Zulassung eines neuen Produkts: Aufgaben des TBV	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_6535	Zulassung eines geänderten Produkts: Aufgaben des TBV	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
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_4182	Kennzeichnung von personen- bzw. organisationsbezogenen Zertifikaten	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_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_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_5083	Zertifikatsantragstellung im Vier-Augen-Prinzip	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_4208	Ausgabe von Zertifikaten	gemRL_TSL_SP_CP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4209	Sicherstellung der Verbindung von Zertifikatsnehmer und privatem Schlüssel	gemRL_TSL_SP_CP
GS-A_4394	Dokumentation der Zertifikatsausgabeprozesse	gemRL_TSL_SP_CP
GS-A_4906	Zuordnung von Schlüsseln zu Identitäten	gemRL_TSL_SP_CP
GS-A_4395	Benachrichtigung des Zertifikatsnehmer	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
GS-A_4214	Veröffentlichung der öffentlichen Schlüssel durch den TSP-X.509 nonQES	gemRL_TSL_SP_CP
GS-A_4348	Verbot der Erneuerung von Zertifikaten	gemRL_TSL_SP_CP
GS-A_4215	Bedingungen für eine Zertifizierung nach Schlüsselerneuerung	gemRL_TSL_SP_CP
GS-A_4216	Bedingungen für eine Zertifikatsänderung	gemRL_TSL_SP_CP
GS-A_4217	Autorisierung einer Zertifikatsänderung	gemRL_TSL_SP_CP
GS-A_4218	Beschreibung der Bedingungen für die Sperrung eines Anwenderzertifikats	gemRL_TSL_SP_CP
GS-A_4219	Sperrung von Anwenderzertifikaten	gemRL_TSL_SP_CP
GS-A_4221	Anzeige der Kompromittierung des privaten Signaturschlüssels	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_4225	Festlegung eines Sperrberechtigten für Endanwenderzertifikate	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_4228	Unverzügliche Bearbeitung eines Sperrantrags	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_5084	Zugang zu HSM-Systemen im Vier-Augen-Prinzip	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
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 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_4332	Dokumentation der Pflichten des Antragstellers eines Komponentenzertifikats	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	gemRL_TSL_SP_CP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Testzertifikate	
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_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_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_4930	CP-Test, Verfügbarkeit des Statusabfragedienstes	gemRL_TSL_SP_CP
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4831	Standards für IPv4	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_4018	Dokumentation UDP/TCP-Portbereiche Anbieter	gemSpec_Net
GS-A_4027	Reporting IP-Adressbereiche	gemSpec_Net
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_3824	FQDN von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform	gemSpec_Net
GS-A_4810	DNS-SD, Format von TXT Resource Records	gemSpec_Net
GS-A_3931	DNSSEC-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS-A_4820	Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform	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_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	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_5039	Änderung der Produktversion bei Änderungen der	gemSpec_OM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Produkttypversion	
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	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_4149	Performance - Reporting-Daten in Performance-Report	gemSpec_Perf
GS-A_4155	Performance - zentrale Dienste - Verfügbarkeit	gemSpec_Perf
GS-A_5028	Performance - zentrale Dienste - Verfügbarkeit Produktivbetrieb	gemSpec_Perf
GS-A_3055	Performance - zentrale Dienste - Skalierbarkeit (Anbieter)	gemSpec_Perf
GS-A_3058	Performance - zentrale Dienste - lineare Skalierbarkeit	gemSpec_Perf
GS-A_4159	Performance – OCSP Responder – Bearbeitungszeiten unter Spitzenlast	gemSpec_Perf
GS-A_4257	Hauptsitz und Betriebsstätte	gemSpec_PKI
GS-A_5511	Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 nonQES	gemSpec_PKI
GS-A_5528	Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 nonQES	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_4828	Vorgaben zur Bildung von nonQES-CA-Namen	gemSpec_PKI
GS-A_4584	Verwendung von Berufsgruppenkennzeichen	gemSpec_PKI
GS-A_4901	Einheitliche Admission in Zertifikaten einer Karte	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_4588	CA-Namen für Test-PKI der TI	gemSpec_PKI
GS-A_5337	Größenbeschränkung von X.509 Zertifikaten auf Karten	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_4737	Umsetzung nonQES-CA-Zertifikate	gemSpec_PKI
GS-A_4739	Attribute der OCSP-Signer-Zertifikate	gemSpec_PKI
GS-A_5514	Verwendung separater OCSP-Signer-Zertifikate	gemSpec_PKI
GS-A_4740	Zentrale OCSP-Signer-CA-Zertifikate	gemSpec_PKI
GS-A_4935	Eindeutige Identifizierung der CRL-Signer-Zertifikate	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4685	Statusprüfdienst - Steigerung der Performance	gemSpec_PKI
GS-A_4687	Statusprüfdienst - Response Status sigRequired	gemSpec_PKI
GS-A_4689	Statusprüfdienst - Zeitquelle von producedAt	gemSpec_PKI
TIP1-A_5994	Störungsampel und Client, I_Monitoring_Update, eindeutige Zuordnung	gemSpec_St_Ampel
TIP1-A_5995	Störungsampel und Client, I_Monitoring_Update, Servicepunkte und IP-Adressen	gemSpec_St_Ampel
TIP1-A_6003	Nutzer der Störungsampel I_Monitoring_Update, eindeutige Zuordnung des Messwertes	gemSpec_St_Ampel
TIP1-A_5999	Nutzer der Störungsampel I_Monitoring_Update, maximale HTTP-Nachrichtenlänge	gemSpec_St_Ampel
TIP1-A_3547	Erstellung einer Ausgabepolicy	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_5088	Sektorzulassung für zugelassene TSP-X.509	gemSpec_X.509_TSP
TIP1-A_3880	Bestätigung Auflagen bei Widerruf der Zulassung	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_3630	Implementierung eines Sperrdienstes für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_5376	Erreichbarkeit des Sperrdienstes von TSP-X.509 nonQES und gematik Root-CA	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_3555	Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA	gemSpec_X.509_TSP
TIP1-A_3558	Schnittstellen TSP-X.509 nonQES für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3564	Bereitstellung eines Registrierungsdienstes	gemSpec_X.509_TSP
TIP1-A_3565	Certificate Policy des TSP-X.509 nonQES	gemSpec_X.509_TSP
TIP1-A_3567	Abgestimmtes Antragsverfahren zwischen TSP-X.509 nonQES und Kartenherausgeber	gemSpec_X.509_TSP
TIP1-A_3569	Weiterleitung von Zertifikatsanträgen an Registrierungsdienst	gemSpec_X.509_TSP
TIP1-A_5089	Negative Prüfung von nonQES-Zertifikatsanträgen	gemSpec_X.509_TSP
TIP1-A_5086	Eingangsdaten der Bestätigungsprüfende Stelle für Produktion von nonQES-Zertifikaten für Leistungserbringer	gemSpec_X.509_TSP
TIP1-A_3580	Übermittlung der Antragsdaten an Erstellungsdienst	gemSpec_X.509_TSP
TIP1-A_3581	Ausgangsdaten für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_5090	Rückmeldung Zertifikatsinformationen (nonQES) an Bestätigende Stelle	gemSpec_X.509_TSP
TIP1-A_3884	Umgang mit nicht-sicherheitskritischen Incidents für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3582	Umsetzung Registrierungsdienst TSP-X.509 nonQES für	gemSpec_X.509_TSP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Personen- und Organisationszertifikate	
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_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_3596	Umsetzung Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3631	Prüfung der Berechtigung des Antragstellers für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3632	Angaben des Sperrantrags für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3633	Identifizierung des zu sperrenden nonQES-Personen- und Organisationszertifikates	gemSpec_X.509_TSP
TIP1-A_3634	Eingangsdaten zur Identifizierung des nonQES-Personen- und Organisationszertifikates	gemSpec_X.509_TSP
TIP1-A_3635	Regelungen zum Sperrprozess für nonQES-Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_3638	Unmittelbare Ausführung der Sperrung von nonQES-Personen- und Organisationszertifikaten	gemSpec_X.509_TSP
TIP1-A_3642	Umsetzung der Schnittstelle des Sperrdienstes für Personen- und Organisationszertifikate	gemSpec_X.509_TSP
TIP1-A_4467	Prüfung der Sperrberechtigung für nonQES-HBA- und Organisationszertifikate	gemSpec_X.509_TSP

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach ITSEC [ITSEC] oder 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 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

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
GS-A_4906	Zuordnung von Schlüsseln zu Identitäten	gemRL_TSL_SP_CP
GS-A_4230	Gewährleistung der Online-Verfügbarkeit von Sperrinformationen	gemRL_TSL_SP_CP
GS-A_4396	Speicherung hinterlegter Root- und CA-Schlüssel	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	gemRL_TSL_SP_CP

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Generierung von Schlüsseln	
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_4925	CP-Test, Keine Verwendung von Echtdaten	gemRL_TSL_SP_CP
GS-A_4435	kDSM: Dokumentation des DSM	gemSpec_DSM
GS-A_4437	kDSM: Jährliche Prüfung der Dokumentation des DSM	gemSpec_DSM
GS-A_4451	kDSM: Kein Personenbezug in Kennzahlen	gemSpec_DSM
GS-A_4453	kDSM: Sicherstellung der Kennzahl-Meldung in Unterbeauftragungsverhältnissen	gemSpec_DSM
GS-A_4473	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß § 42a BDSG bzw. § 83a SGB X	gemSpec_DSM
GS-A_4474	kDSM: Nutzung des Incident Managements der gematik	gemSpec_DSM
GS-A_4475	kDSM: Stellungnahme bei gravierenden Datenschutzverstößen gemäß § 42a BDSG bzw. § 83a SGB X	gemSpec_DSM
GS-A_4480	kDSM: Berücksichtigung von Änderungen im Datenschutzrecht und Ergebnissen des technischen Fortschritts	gemSpec_DSM
GS-A_4503	Dokumentation des ISM	gemSpec_ISM
GS-A_4505	Jährliche Prüfung der Dokumentation des ISM	gemSpec_ISM
GS-A_4529	Meldung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4537	Meldung von Informationssicherheitsrisiken	gemSpec_ISM
GS-A_4539	Meldung von angepassten Risikoleveln	gemSpec_ISM
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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4386	TLS-Verbindungen, optional Version 1.1	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	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_5131	Hash-Algorithmus bei OCSP / CertID	gemSpec_Krypt
GS-A_5079	Migration von Algorithmen und Schlüssellängen bei PKI-Betreibern	gemSpec_Krypt
GS-A_4062	Sicherheitskomponenten bei Netzübergängen zu Fremdnetzen	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_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
GS-A_3760	Gutachten zur Einhaltung der Sicherheitsanforderungen für Dienstbetreiber	gemSpec_SiBetrUmg
GS-A_4980	Umsetzung der Norm ISO/IEC 27001	gemSpec_SiBetrUmg
GS-A_4981	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_SiBetrUmg
GS-A_4982	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_SiBetrUmg
GS-A_4983	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_SiBetrUmg
GS-A_4984	Befolgen von herstellerspezifischen Vorgaben	gemSpec_SiBetrUmg
GS-A_3737	Spezifisches Sicherheitskonzept: Mindestumfang des spezifischen Sicherheitskonzeptes..	gemSpec_SiBetrUmg
GS-A_3747	Technische_Komponenten: Dokumentation der technischen Komponenten und der geforderten Sicherheitsfunktionalität.	gemSpec_SiBetrUmg
GS-A_3753	Notfallkonzept: Der Dienstanbieter muss ein Notfallkonzept erstellen	gemSpec_SiBetrUmg
GS-A_3772	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_SiBetrUmg
GS-A_3756	Umsetzung_Maßnahmen_spezifisches_Siko: Umsetzung und Prüfbarkeit von Maßnahmen	gemSpec_SiBetrUmg
GS-A_2214	Anbieter müssen jährlich die Betreiber kontrollieren.	gemSpec_Sich_DS
GS-A_2087	Information für Betroffene über Produkte durch Anbieter und	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Betreiber	
GS-A_2213	Wahrnehmung der Betroffenenrechte beim Anbieter	gemSpec_Sich_DS
GS-A_2076	Datenschutzmanagement nach BSI für Betreiber	gemSpec_Sich_DS
GS-A_2174	Inhalte des Sicherheitsgutachtens aus Sicht des Datenschutzes	gemSpec_Sich_DS
GS-A_2177	Anbieter müssen Pflichten der Auftragsdatenverarbeitung erfüllen	gemSpec_Sich_DS
GS-A_2012	Verantwortung der Anbieter und Betreiber für Einhaltung der Anforderungen Datenschutz und Informationssicherheit	gemSpec_Sich_DS
GS-A_2021	Anwendung der einheitlichen Methoden der Informationssicherheit durch Betreiber und Anbieter	gemSpec_Sich_DS
GS-A_2046	Umsetzung der Anforderungen aus [gemSpec_SiBetrUmg] durch Anbieter von zentralen Produkten	gemSpec_Sich_DS
GS-A_4944	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_Sich_DS
GS-A_4945	Produktentwicklung: Qualitätssicherung	gemSpec_Sich_DS
GS-A_4946	Produktentwicklung: sichere Programmierung	gemSpec_Sich_DS
GS-A_4947	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_Sich_DS
GS-A_2047	Gestaltung der Umgebung von zentralen Produkten durch Betreiber für Schutzbedarf "mittel"	gemSpec_Sich_DS
GS-A_2309	ISM der Beteiligten: Rollen und Verantwortlichkeiten	gemSpec_Sich_DS
GS-A_2326	ISM der Beteiligten: Etablierung	gemSpec_Sich_DS
GS-A_2328	ISM der Beteiligten: Pflege und Fortschreibung der Sicherheitskonzepte	gemSpec_Sich_DS
GS-A_2329	ISM der Beteiligten: Umsetzung der Sicherheitskonzepte	gemSpec_Sich_DS
GS-A_2330	ISM der Beteiligten: Schwachstellen-Management	gemSpec_Sich_DS
GS-A_2331	ISM der Beteiligten: Sicherheitsvorfalls-Management	gemSpec_Sich_DS
GS-A_2332	ISM der Beteiligten: Notfallmanagement	gemSpec_Sich_DS
GS-A_2333	ISM der Beteiligten: Meldung an das koordinierende ISM	gemSpec_Sich_DS
GS-A_2339	ISM der Beteiligten: regelmäßige Reviews	gemSpec_Sich_DS
GS-A_2343	ISM der Beteiligten: eigene Audits	gemSpec_Sich_DS
GS-A_2345	ISM der Beteiligten: Reviews und Trendanalysen	gemSpec_Sich_DS
GS-A_2347	ISM der Beteiligten: Grundlagen neuer Planungsphasen	gemSpec_Sich_DS
GS-A_2360	ISM der Beteiligten: Meldung von Restrisiken	gemSpec_Sich_DS
GS-A_2361	ISM der Beteiligten: Vorfallsmanagement	gemSpec_Sich_DS
GS-A_2362	ISM der Beteiligten: Bericht lokaler Sicherheitsvorfälle	gemSpec_Sich_DS
GS-A_2363	ISM der Beteiligten: Meldung schwerwiegender Sicherheitsvorfälle	gemSpec_Sich_DS
GS-A_2366	ISM der Beteiligten: Notfallbewältigung	gemSpec_Sich_DS
GS-A_3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	gemSpec_Sich_DS
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_Sich_DS
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_Sich_DS
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	gemSpec_Sich_DS
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	gemSpec_Sich_DS
TIP1-A_5087	Berücksichtigung und Umsetzung übergeordneter Herausgeberpolicies	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-Zertifikatstatusinformationen, Zertifikats- und Sperranträge	gemSpec_X.509_TSP
TIP1-A_4234	Protokollierung von OCSP-Anfragen	gemSpec_X.509_TSP
TIP1-A_4235	Fehlerprotokollierung	gemSpec_X.509_TSP
TIP1-A_3660	Trennung der TSP-X.509-Betriebsumgebungen	gemSpec_X.509_TSP
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_3881	Schutzbedarf darf nicht verringert werden	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_3590	Eindeutige Verbindung Personen- und Organisationszertifikatsnehmer und privater Schlüssel	gemSpec_X.509_TSP
TIP1-A_3595	Anforderungen von LEO- und KTR-Institutionen	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

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 6: nicht nachzuweisende Anforderungen

GS-A_4173	GS-A_4275	GS-A_4305	GS-A_4435	GS-A_3772	GS-A_2309	GS-A_3139
GS-A_4191	GS-A_4276	GS-A_4306	GS-A_4437	GS-A_4980	GS-A_2326	GS-A_3141
GS-A_4230	GS-A_4279	GS-A_4307	GS-A_4451	GS-A_4981	GS-A_2328	GS-A_3149
GS-A_3130	GS-A_4284	GS-A_4308	GS-A_4453	GS-A_4982	GS-A_2329	GS-A_4944
GS-A_4249	GS-A_4285	GS-A_4309	GS-A_4480	GS-A_4983	GS-A_2330	GS-A_4945
GS-A_4255	GS-A_4287	GS-A_4310	GS-A_4503	GS-A_4984	GS-A_2331	GS-A_4946
GS-A_4259	GS-A_4288	GS-A_4311	GS-A_4505	GS-A_2012	GS-A_2332	GS-A_4947
GS-A_4261	GS-A_4289	GS-A_4312	GS-A_4367	GS-A_2046	GS-A_2345	TIP1-A_3548
GS-A_4268	GS-A_4290	GS-A_4313	GS-A_4368	GS-A_2047	GS-A_2347	TIP1-A_3550
GS-A_4270	GS-A_4291	GS-A_4314	GS-A_3737	GS-A_2076	GS-A_2361	TIP1-A_3554
GS-A_4271	GS-A_4292	GS-A_4315	GS-A_3747	GS-A_2087	GS-A_2366	TIP1-A_4230
GS-A_4272	GS-A_4294	GS-A_4316	GS-A_3753	GS-A_2174	GS-A_3078	TIP1-A_4235
GS-A_4273	GS-A_4295	GS-A_4317	GS-A_3756	GS-A_2177	GS-A_3125	
GS-A_4274	GS-A_4304	GS-A_4906	GS-A_3760	GS-A_2214		

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 7: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4436	kDSM: Bereitstellung der Dokumentation des DSM bei Audits	gemSpec_DSM
GS-A_4448	kDSM: Übermittlung von Reports	gemSpec_DSM
GS-A_4449	kDSM: Monatliche Reports in der Erprobung	gemSpec_DSM
GS-A_4450	kDSM: Erfassungszeitraum monatlicher Reports	gemSpec_DSM
GS-A_4455	kDSM: Anpassung der Reports bei geänderten Kennzahlen	gemSpec_DSM
GS-A_4456	kDSM: Dateiformat des Kennzahlen-Reports	gemSpec_DSM
GS-A_4457	kDSM: Anpassung an geändertes CSV-Format	gemSpec_DSM
GS-A_4458	kDSM: Identifizierung der Ursachen von auffälligen Kennzahlenwerten	gemSpec_DSM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4459	kDSM: Meldung der Anzahl der Datenschutzbeschwerden	gemSpec_DSM
GS-A_4460	kDSM: Meldung der Anzahl der Datenschutzanfragen	gemSpec_DSM
GS-A_4461	kDSM: Meldung der fehlerhaft adressierten Datenschutzanfragen	gemSpec_DSM
GS-A_4462	kDSM: Durchschnittliche Bearbeitungszeit für Datenschutzanfragen	gemSpec_DSM
GS-A_4463	kDSM: Meldung der Anzahl gravierender Datenschutzvorfälle	gemSpec_DSM
GS-A_4464	kDSM: Meldung der Datenschutzschulungstage	gemSpec_DSM
GS-A_4465	kDSM: Meldung des Anteils der Verfahren im internen Verfahrensverzeichnis	gemSpec_DSM
GS-A_4466	kDSM: Meldung der Anzahl externer und interner Datenschutz-Audits	gemSpec_DSM
GS-A_4467	kDSM: Selbsteinschätzung zum Datenschutz	gemSpec_DSM
GS-A_4468	kDSM: Jährlicher Datenschutzreport der TI	gemSpec_DSM
GS-A_4470	kDSM: Informationen zu Kennzahlen im Datenschutzreport der TI	gemSpec_DSM
GS-A_4471	kDSM: Auftragsdatenverarbeitung im Datenschutzreport der TI	gemSpec_DSM
GS-A_4476	kDSM: Maßnahmen zur Behebung gravierender Datenschutzverstöße	gemSpec_DSM
GS-A_4477	kDSM: Umgehende Umsetzung von Maßnahmen bei gravierenden Datenschutzverstößen	gemSpec_DSM
GS-A_4478	kDSM: Kontrolle der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes	gemSpec_DSM
GS-A_4479	kDSM: Meldung von Kontaktinformationen zum Datenschutzmanagement	gemSpec_DSM
GS-A_4481	kDSM: Berücksichtigung von Änderungen der Datenschutzanforderungen der TI	gemSpec_DSM
GS-A_4482	kDSM: Kontrolle der Umsetzung von Maßnahmen durch die gematik	gemSpec_DSM
GS-A_4504	Bereitstellung der Dokumentation des ISM bei Audits	gemSpec_ISM
GS-A_4506	Übermittlung von Security Reports	gemSpec_ISM
GS-A_4507	Bereitstellung des Security Reports in der Erprobung	gemSpec_ISM
GS-A_4508	Bereitstellung des Security Reports im Produktivbetrieb	gemSpec_ISM
GS-A_4509	Dateiformat und -struktur des Security Reports	gemSpec_ISM
GS-A_4511	Aufschlüsselung pro TI-Produkt	gemSpec_ISM
GS-A_4512	Dateistruktur der Informationen in den Security Reports	gemSpec_ISM
GS-A_4513	Kennzahl 01: Budgetierung der Informationssicherheit	gemSpec_ISM
GS-A_4514	Kennzahl 02: Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter	gemSpec_ISM
GS-A_4515	Kennzahl 03: Anzahl der externen und internen Informationssicherheits-Audits	gemSpec_ISM
GS-A_4516	Kennzahl 04: Behebungszeit von in internen oder externen Audits festgestellten Abweichungen	gemSpec_ISM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4517	Kennzahl 05: Vollständigkeit der Erfassung organisationseigener Werte (Assets)	gemSpec_ISM
GS-A_4518	Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management)	gemSpec_ISM
GS-A_4519	Kennzahl 7 Anteil sicherheitsrelevanter Änderungen (Security Changes)	gemSpec_ISM
GS-A_4520	Kennzahl 08: Anzahl privilegierter Benutzer	gemSpec_ISM
GS-A_4521	Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen	gemSpec_ISM
GS-A_4522	Kennzahl 10: Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter	gemSpec_ISM
GS-A_4523	Bereitstellung Kommunikationsschnittstelle für Informationssicherheit	gemSpec_ISM
GS-A_4524	Meldung von Kontaktinformationen zum Informationssicherheitsmanagement	gemSpec_ISM
GS-A_4525	Audit-Unterstützung des Koordinators für Informationssicherheit	gemSpec_ISM
GS-A_4526	Aufbewahrungsvorgaben an die Nachweise zu den im Security Report gemachten Angaben	gemSpec_ISM
GS-A_4527	Audit-Kennzahlen	gemSpec_ISM
GS-A_4528	Meldung von lokalen Sicherheitsvorfällen	gemSpec_ISM
GS-A_4530	Maßnahmen zur Behebung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4531	Unverzügliche Umsetzung von Maßnahmen bei schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4532	Kontrolle der Umsetzung von Maßnahmen in Folge eines schwerwiegenden Sicherheitsvorfalls oder -notfalls	gemSpec_ISM
GS-A_4533	Berücksichtigung von Änderungen im Umfeld der Informationssicherheit und Ergebnissen des technischen Fortschritts	gemSpec_ISM
GS-A_4534	Berücksichtigung von Änderungen der Informationssicherheitsanforderungen der TI	gemSpec_ISM
GS-A_4535	Kontrolle der Umsetzung von Maßnahmen durch die gematik	gemSpec_ISM
GS-A_4538	Nutzen des Risikobewertungstemplate	gemSpec_ISM
GS-A_4540	Risikoreporting	gemSpec_ISM
GS-A_5541	TLS-Verbindungen als TLS-Klient zur Störungsampel	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_5518	Prüfung Kurvenpunkte bei einer Zertifikatserstellung	gemSpec_Krypt
GS-A_4965	Keine Suspendierung von X.509-Zertifikaten (außer für eGK)	gemSpec_PKI
GS-A_3784	Nachweis durch ISO27001 Zertifikat	gemSpec_SiBetrUmg
GS-A_5324	Teilnahme des Anbieters an Sitzungen des kDSMS/kISMS	gemSpec_Sich_DS
GS-A_2355	ISM der Beteiligten: Nutzung des Problem-Management-Prozesses	gemSpec_Sich_DS
GS-A_2356	ISM der Beteiligten: Nutzung des Incident-Management-	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Prozesses	
GS-A_2357	ISM der Beteiligten: Nutzung der Prozesse und Reports des Betriebs	gemSpec_Sich_DS
GS-A_2359	ISM der Beteiligten: Nutzung der Sicherheits-Technologien des koordinierenden ISM	gemSpec_Sich_DS

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

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

4 Produkttypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produkttyps vor.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

A2 – Tabellenverzeichnis

A3 – Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[BSI_2006a]	BSI (29.09.2006): Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria) https://www.bsi.bund.de/Schutzprofile
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[ITSEC]	BMI bzw. GMBl: (28.06.1991): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik („Information Technology Security Evaluation Criteria“) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile
[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

[Quelle]	Herausgeber: Titel, Version
	zur Aufhebung der Richtlinie 1999/93/EG