Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

OCSP-Responder-Proxy

Produkttyp Version:	2.4.0-1
Produkttyp Status:	freigegeben

Version:	1.0.1
Revision:	249005
Stand:	06.07.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_OCSP_Proxy_PTV_2.4.0-1

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_OCSP_Proxy_PTV1.0.0
1.1.0	Losübergreifende Synchronisation	gemProdT_OCSP_Proxy_PTV1.1.0
1.2.0	P11-Änderungsliste	gemProdT_OCSP_Proxy_PTV1.2.0
1.2.1	P12-Änderungsliste	gemProdT_OCSP_Proxy_PTV1.2.1
1.4.0	Änderungen aus Errata 1.4.3 und 1.4.6 eingefügt	gemProdT_OCSP_Proxy_PTV1.4.0
1.5.0	Anpassung OPB1	gemProdT_OCSP_Proxy_PTV1.5.0
2.0.0	Anpassung R1.6.3	gemProdT_OCSP_Proxy_PTV2.0.0
2.0.0-0	Anpassung auf Releasestand 1.6.3	gemProdT_OCSP_Proxy_PTV2.0.0-0
2.0.0-1	Anpassung auf Releasestand 1.6.4	gemProdT_OCSP_Proxy_PTV2.0.0-1
2.1.0-0	Anpassung an Releasestand 2.1.2	gemProdT_OCSP_Proxy_PTV2.1.0-0
2.2.0-0	Anpassung an Releasestand 2.1.3	gemProdT_OCSP_Proxy_PTV2.2.0-0
2.3.0-0	Anpassung an Releasestand 3.1.0	gemProdT_OCSP_Proxy_PTV2.3.0-0
2.4.0-0	Anpassung an Releasestand 3.1.2	gemProdT_OCSP_Proxy_PTV2.4.0-0
2.4.0-1	Anpassung an Releasestand 4.0.0	gemProdT_OCSP_Proxy_PTV2.4.0-1

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	30.06.20		freigegeben	gematik
1.0.1	06.07.20		GS-A_4147 und GS-A_4148 entfernt	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps OCSP-Responder-Proxy oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung" verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.).

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an OCSP-Responder-Proxy-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

1.3 Geltungsbereich

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

1.4 Abgrenzung des Dokumentes

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

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

1.5 Methodik

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

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

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

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.9.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.18.0
gemSpec_OCSP_Proxy	Spezifikation OCSP-Proxy	1.9.0
gemSpec_ServiceMon	Spezifikation Service Monitoring	1.5.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.17.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.2.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.14.0
gemKPT_Test	Testkonzept der TI	2.7.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.11.0

Errata

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

3 Blattanforderungen

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

3.1 Anforderungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS−A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS−A_4829	TUCs, Fehlerbehandlung	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_17820	Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)	gemSpec_PKI
A_17821	Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)	gemSpec_PKI
GS−A_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
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	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_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS−A_4899	TSL Update-Prüfintervall	gemSpec_PKI
A_17700	TSL-Auswertung ServiceTypeIdentifier "unspecified"	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_4660−01	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS−A_4749−01	TUC_PKI_007: Prüfung Zertifikatstyp	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_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_4957−01	Beschränkungen OCSP-Request	gemSpec_PKI
GS−A_4832	Path MTU Discovery und ICMP Response	gemSpec_Net
A_17824	Zentrale Dienste der TI-Plattform, Nutzung von IPv6	gemSpec_Net
GS−A_4036	Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen	gemSpec_Net
GS−A_4763	Einsatz von Hochverfügbarkeitsprotokollen	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_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
TIP1−A_5848	Erreichbarkeit OCSP-Proxy	gemSpec_OCSP_Proxy
TIP1−A_5849	OCSP-Anfragen aus der TI beantworten	gemSpec_OCSP_Proxy
TIP1−A_5851	Weiterleitung von OCSP-Anfragen für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten.	gemSpec_OCSP_Proxy
TIP1−A_5853	Ablehnung von Anfragen aus dem Internet	gemSpec_OCSP_Proxy
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 Nachrichtenübermittelung	gemSpec_ServiceMon

TIP1−A_7126	Nutzer des Service Monitorings I_Monitoring_Update, Zeitstempel bei Ausfall/Wiederherstellung	gemSpec_ServiceMon
TIP1−A_7128	Nutzer des Service Monitorings I_Monitoring_Update, maximale HTTP-Nachrichtenlänge	gemSpec_ServiceMon
A_15166	Nutzer der Schnittstelle I_Monitoring_Update, Zertifikatsprüfung	gemSpec_ServiceMon
GS−A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
GS−A_3695	Grundlegender Aufbau Versionsnummern	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_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS−A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS−A_4543	Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten	gemSpec_OM
GS−A_4545	Kurzform der Selbstauskunft für zentrale Produkttypen der TI-Plattform und fachanwendungsspezifische Dienste an die Störungsampel	gemSpec_OM
GS−A_4146−01	Performance – Performance-Daten erfassen	gemSpec_Perf
A_14936	Performance - Störungsampel - Ereignisnachricht bei Ausfall zentrale Dienste	gemSpec_Perf
GS−A_4149−01	Performance – Reporting-Daten in Performance-Report	gemSpec_Perf
A_17757−01	Performance - Rohdaten-Performance-Lieferung - zu liefernde Dateien	gemSpec_Perf
GS−A_4145	Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen	gemSpec_Perf

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante

Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS−A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
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_4013	Nutzung von UDP/TCP-Portbereichen	gemSpec_Net
GS−A_4018	Dokumentation UDP/TCP-Portbereiche Anbieter	gemSpec_Net
GS−A_4024	Nutzung IP-Adressbereiche	gemSpec_Net
GS−A_4027	Reporting IP-Adressbereiche	gemSpec_Net
GS−A_4759	IPv4-Adressen Produkttyp zum SZZP	gemSpec_Net
GS−A_4033	Statisches Routing TI-Übergabepunkte	gemSpec_Net
GS−A_4054	Paketfilter Default Deny	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_3931	DNSSEC-Protokoll, Nameserver-Implementierungen	gemSpec_Net
GS−A_4820	Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform	gemSpec_Net
TIP1−A_5831	FehlerLog	gemSpec_OCSP_Proxy
TIP1−A_5835	Fehlerprotokollierung	gemSpec_OCSP_Proxy

TIP1−A_5838	Verwendung von Standards und Best Practices	gemSpec_OCSP_Proxy
TIP1−A_5852	Verbindungsaufbau zu OCSP-Respondern im Internet	gemSpec_OCSP_Proxy
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
GS−A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS−A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
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_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS−A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS−A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM

GS−A_5018	Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen	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_5033	Betriebsdokumentation der zentralen Produkte der TI-Plattform und anwendungsspezifischen Diensten	gemSpec_OM
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_7358	Qualität des Produktmusters	gemKPT_Test
TIP1−A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1−A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1−A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
GS−A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	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_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1−A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1−A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1−A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1−A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1−A_6085	Referenzobjekte eines Produkts	gemKPT_Test

TIP1−A_2805	Zeitnahe Anpassung von Produktkonfigurationen	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_7333	Parallelbetrieb von Release oder Produkttypversion	gemKPT_Test
TIP1−A_7334	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
TIP1−A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1−A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1−A_6524−01	Testdokumentation gemäß Vorlagen	gemKPT_Test
A_20065	Nutzung der Dokumententemplates der gematik	gemKPT_Test
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

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria (CC) ist nicht erforderlich.

3.2.2 Sicherheitsgutachten

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

Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS−A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS−A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
GS−A_4054	Paketfilter Default Deny	gemSpec_Net
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
TIP1−A_5836	Schutz von Log-Dateien	gemSpec_OCSP_Proxy
TIP1−A_5837	Technische Datenschutzmaßnahmen	gemSpec_OCSP_Proxy
TIP1−A_5853	Ablehnung von Anfragen aus dem Internet	gemSpec_OCSP_Proxy
TIP1−A_5855	Speicherung von OCSP-Anfragen	gemSpec_OCSP_Proxy
TIP1−A_5856	Speicherung von OCSP-Antworten	gemSpec_OCSP_Proxy
TIP1−A_5857	Protokollierung von OCSP-Anfragen und OCSP-Antworten	gemSpec_OCSP_Proxy
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_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht 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_4388	DNSSEC-Kontext	gemSpec_Krypt
GS−A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
GS−A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS−A_4980−01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS−A_4981−01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS−A_4982−01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS−A_4983−01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS−A_3737−01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS−A_3753−01	Notfallkonzept	gemSpec_DS_Anbieter
GS−A_3772−01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS−A_2328−01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS−A_2329−01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS−A_2345−01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS−A_2158−01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS−A_4984−01	Befolgen von herstellerspezifischen Vorgaben	gemSpec_DS_Anbieter
GS−A_2331−01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS−A_2332−01	Notfallmanagement	gemSpec_DS_Anbieter
GS−A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS−A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS−A_2076−01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS−A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
GS−A_2214−01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	gemSpec_DS_Anbieter

3.2.3 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_18467	TLS-Verbindungen, Version 1.3	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_5526	TLS-Renegotiation-Indication-Extension	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
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_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS−A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS−A_2355−01	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS−A_5559	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS−A_5017−01	Meldung und Behandlung von Schwachstellen	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_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_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS−A_4526−01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS−A_5564	kDSM: Ansprechpartner für Datenschutz	gemSpec_DS_Anbieter
GS−A_4479−01	kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement	gemSpec_DS_Anbieter
GS−A_4473−01	kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
GS−A_5565	kDSM: Unverzügliche Behebung von 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_5324−02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter
GS−A_4468−02	kDSM: Jährlicher Datenschutzbericht der TI	gemSpec_DS_Anbieter
GS−A_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS−A_5625	kDSM: Auditrechte der gematik zum Datenschutz	gemSpec_DS_Anbieter

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.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig]	gematik:Richtlinie zur Prüfung der Sicherheitseignung