Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Identity Provider - Dienst

Produkttyp Version:	1.0.0-0
Produkttyp Status:	freigegeben

Version:	1.0.0
Revision:	247419
Stand:	30.06.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_IDP-Dienst_PTV_1.0.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version auf Dokumentenebene	gemProdT_IDP-Dienst_PTV_1.0.0-0

Historie Produkttypsteckbrief

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

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	30.06.20		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung 4

1.1 Zielsetzung und Einordnung des Dokumentes 4

1.2 Zielgruppe 4

1.3 Geltungsbereich 4

1.4 Abgrenzung des Dokumentes 4

1.5 Methodik 5

2 Dokumente 6

3 Blattanforderungen 7

3.1 Anforderungen zur funktionalen Eignung 7

3.1.1 Produkttest/Produktübergreifender Test 7

3.1.2 Herstellererklärung funktionale Eignung 14

3.2 Anforderungen zur sicherheitstechnischen Eignung 19

3.2.1 Herstellererklärung sicherheitstechnische Eignung 19

3.2.2 Sicherheitsgutachten 22

3.2.3 Produktgutachten 23

4 Anhang – Verzeichnisse 28

4.1 Abkürzungen 28

4.2 Tabellenverzeichnis 28

4.3 Referenzierte Dokumente 28

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 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 Hersteller des IdP-Dienstes sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 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_IDP_Dienst	Spezifikation Identity Provider - Dienst	1.0.0
gemSpec_IDP_FD	Spezifikation Identity Provider – Fachdienste	1.0.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.11.0
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.7.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.17.0
gemKPT_Test	Testkonzept der TI	2.7.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.2.0
gemSpec_SST_LD_BD	Spezifikation Logdaten und Betriebsdatenerfassung	1.2.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.14.0

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
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_4943	Alter der OCSP-Responses für eGK-Zertifikate	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_4957−01	Beschränkungen OCSP-Request	gemSpec_PKI
GS−A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
A_19881	Gültigkeitsdauer von JSON-Schlüsselmaterial	gemSpec_IDP_Dienst
A_19870	Verwendung eindeutiger URI	gemSpec_IDP_Dienst

A_19871	Bekanntgabe des Downloadpunktes im Fachportal der gematik	gemSpec_IDP_Dienst
A_19872	Discovery Document interne und externe Adressierung	gemSpec_IDP_Dienst
A_19873	Inhalte des Discovery Documents	gemSpec_IDP_Dienst
A_19874	Bereitstellung Internes Discovery Document innerhalb der TI	gemSpec_IDP_Dienst
A_19875	Absicherung des Internen Discovery Document innerhalb der TI mit TLS	gemSpec_IDP_Dienst
A_19876	Internes Discovery Document - Prüfung vor Veröffentlichung	gemSpec_IDP_Dienst
A_19877	Bereitstellung Externes Discovery Document im Internet	gemSpec_IDP_Dienst
A_19878	Absicherung des Externen Discovery Document im Internet mit TLS	gemSpec_IDP_Dienst
A_19879	Externes Discovery Document - Prüfung vor Veröffentlichung	gemSpec_IDP_Dienst
A_19880	Bereitstellung der PUK	gemSpec_IDP_Dienst
A_19895	Erweiterte Nutzung von Schlüsseln	gemSpec_IDP_Dienst
A_19896	Format der Fehlermeldungen	gemSpec_IDP_Dienst
A_19894	Dynamische Registrierung (Absicherung durch TLS)	gemSpec_IDP_Dienst
A_20145	Das Discovery Document enthält statische Adressen	gemSpec_IDP_Dienst
A_19909	Integrität der Eingangsdaten am Authenticator-Modul	gemSpec_IDP_Dienst
A_20146	Redirection-Endpunkt (Herausgabe von Informationen an Redirection-Endpunkt)	gemSpec_IDP_Dienst
A_20147	Redirection-Endpunkt (Verantwortlichkeit für Aktualität)	gemSpec_IDP_Dienst
A_20148	Discovery Document (Datenbasis Anwendungsfrontend autoclean)	gemSpec_IDP_Dienst
A_20149	Discovery Document (Datenbasis Authenticator autoclean)	gemSpec_IDP_Dienst
A_20150	Das Discovery Document ist maximal 24 Stunden alt	gemSpec_IDP_Dienst

A_20151	Zusätzlicher Schutz des Discovery Documents	gemSpec_IDP_Dienst
A_19860	Der Authorization-Endpunkt Standards	gemSpec_IDP_Dienst
A_19861	Authorization-Endpunkt Authenticator-Modul	gemSpec_IDP_Dienst
A_19862	Authenticator im Apple App Store	gemSpec_IDP_Dienst
A_19863	Schutz vor überalterter Software (Apple)	gemSpec_IDP_Dienst
A_19864	Authenticator im Google Play Store	gemSpec_IDP_Dienst
A_19865	Schutz vor überalterter Software (Android)	gemSpec_IDP_Dienst
A_19853	Protokollierung der Consent-Bestätigung	gemSpec_IDP_Dienst
A_19850	Enschlüsseln der Eingangsdaten am Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19851	Aufbewahrung alter Schlüssel	gemSpec_IDP_Dienst
A_19852	Verwendung des Attributes "auth_time"	gemSpec_IDP_Dienst
A_19848	Verwendung des Attributes "Bearer"	gemSpec_IDP_Dienst
A_19849	ACCESS_CODE und ID_- oder REFRESH_TOKEN nur für gültige Zertifikate	gemSpec_IDP_Dienst
A_19835	Entschlüsselung des Consent	gemSpec_IDP_Dienst
A_19836	Signaturprüfung des Consent	gemSpec_IDP_Dienst
A_19837	Schematische Prüfung des Consent	gemSpec_IDP_Dienst
A_19838	Verarbeitung des Consent	gemSpec_IDP_Dienst
A_19839	Der Authorization-Endpunkt bestätigt ausschließlich Zertifikatsinformationen	gemSpec_IDP_Dienst
A_19840	Inhalte des Claims	gemSpec_IDP_Dienst
A_19841	Maximale Gültigkeitsdauer einer "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19842	Maximale Gültigkeitsdauer des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19843	Maximale Gültigkeitsdauer des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19844	Maximale Gültigkeitsdauer des "ID_TOKEN"	gemSpec_IDP_Dienst
A_19845	Nutzer-Informationen im Claim	gemSpec_IDP_Dienst

A_19977	Keine Token für widerrufene Entitäten	gemSpec_IDP_Dienst
A_19978	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_19846	Signatur des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19847	Verschlüsselung des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19832	Sichere Übertragung des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_20106	Bereitstellung Redirection-Endpunkt	gemSpec_IDP_Dienst
A_20110	Absicherung Redirection-Endpunkt	gemSpec_IDP_Dienst
A_20107	Redirection-Endpunkt Auswertung HTTP-Header	gemSpec_IDP_Dienst
A_20108	Redirection-Endpunkt-Ergänzung mit Portangaben	gemSpec_IDP_Dienst
A_19825	Annahme und Prüfung von "ACCESS_CODE" und "SECRET"	gemSpec_IDP_Dienst
A_19826	"ACCESS_CODE" einmalige Verwendung	gemSpec_IDP_Dienst
A_19827	"ID_TOKEN" Protokollierung in allen Fällen	gemSpec_IDP_Dienst
A_19828	Annahme und Prüfung des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19829	"REFRESH_TOKEN" Protokollierung nur im Negativfall	gemSpec_IDP_Dienst
A_19820	Erfolgreiche Antwort auf "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19821	Signatur des "ID_TOKEN" und "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19822	Verschlüsselung des "ID_TOKEN"	gemSpec_IDP_Dienst
A_19816	Verschlüsselung des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19817	Signatur des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19818	"REFRESH_TOKEN" mathematische und zeitliche Gültigkeit	gemSpec_IDP_Dienst
A_19819	"REFRESH_TOKEN" Integritätsprüfung	gemSpec_IDP_Dienst
A_19809	Sichere Übertragung von "ID_TOKEN" und "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19811	Adressierung der Token beim Versand	gemSpec_IDP_Dienst
A_19812	Token Introspection Timeout	gemSpec_IDP_Dienst

A_19806	Prüfung von "ID_TOKEN" am Introspection-Endpunkt	gemSpec_IDP_Dienst
A_19807	Nur Fachdienste führen Token Introspection durch	gemSpec_IDP_Dienst
A_19808	Inhalte der Token Introspection Antwort	gemSpec_IDP_Dienst
A_19798	Speichern der Token Introspection Antwort (Token Introspection Response Caching)	gemSpec_IDP_Dienst
A_19975	Haltbarkeit der Token Introspection Antwort	gemSpec_IDP_Dienst
A_19799	Die Token Introspection Antwort ist signiert	gemSpec_IDP_Dienst
A_19800	Die Token Introspection Antwort ist verschlüsselt	gemSpec_IDP_Dienst
A_19796	Verwendung von Transport Layer Security (TLS) bei Token Introspection	gemSpec_IDP_Dienst
A_20138	Reaktion auf Fehler bei der Introspection Anfrage	gemSpec_IDP_Dienst
A_19794	Mindestangaben für den Token-Widerruf (Token Revocation minimal information)	gemSpec_IDP_Dienst
A_19795	Token-Widerrufsanfragen sind zu signieren	gemSpec_IDP_Dienst
A_19792	Widerruf des "REFRESH_TOKEN" ("refresh_token" Revocation)	gemSpec_IDP_Dienst
A_19791	Widerruf des "ID_TOKEN" ("id_token" Revocation)	gemSpec_IDP_Dienst
A_19788	Widerruf der "SUBJECT_SESSION" durch Authenticator	gemSpec_IDP_Dienst
A_20018	Widerruf der "SUBJECT_SESSION" durch Fachdienste	gemSpec_IDP_Dienst
A_19789	Widerruf der "SUBJECT_SESSION" durch Backchannel Revocation	gemSpec_IDP_Dienst
A_19790	Backchannel Revocation Information an Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19787	Verwendung terminierter "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19784	Rückmeldung des Status-Code der erfolgreichen Widerrufsumsetzung [RFC7009#section-2.2]	gemSpec_IDP_Dienst
A_19783	Rückmeldung des Status-Code der nicht erfolgten Widerrufsumsetzung	gemSpec_IDP_Dienst

A_19782	Informationen am Userinfo-Endpunkt	gemSpec_IDP_Dienst
A_19750	Keine Verwendung des Attributes "aud"	gemSpec_IDP_FD
A_19751	Inhalte des Claims für Versicherte (eGK)	gemSpec_IDP_FD
A_19752	Inhalte des Claims für Leistungserbringer (HBA)	gemSpec_IDP_FD
A_19753	Inhalte des Claims für SMC-B	gemSpec_IDP_FD
A_19762	Auswertung der positiven Token Introspection	gemSpec_IDP_FD
A_19763	Negative Token Introspection	gemSpec_IDP_FD
A_17757−01	Performance - Rohdaten-Performance-Lieferung - zu liefernde Dateien	gemSpec_Perf
A_17755	Performance - Rohdaten-Performance-Berichte - Name der Berichte	gemSpec_Perf
A_17671	Performance - Rohdaten-Performance-Berichte - Format des Performance-Berichts	gemSpec_Perf
A_17678	Performance - Rohdaten-Performance-Berichte - Übermittlung	gemSpec_Perf
A_17679	Performance - Rohdaten-Performance-Berichte - Berichtsintervall	gemSpec_Perf
A_17756	Performance - Rohdaten-Performance-Berichte - Korrektheit	gemSpec_Perf
A_17758	Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung	gemSpec_Perf
A_19717	Performance – IdP-Dienst – Bearbeitungszeit unter Last	gemSpec_Perf
A_20153	Performance - IdP-Dienst - Anzahl paralleler Sessions - TI	gemSpec_Perf
A_20154	Performance - IdP-Dienst - Anzahl paralleler Sessions - Internet	gemSpec_Perf
A_19501	Funktionsblock App-Check für die Betriebsdatenerfassung	gemKPT_Betr
GS−A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
A_17416−01	Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste	gemSpec_SST_LD_BD

A_17733−01	Schnittstelle Betriebsdatenerfassung Datei-Upload	gemSpec_SST_LD_BD
GS−A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
GS−A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
A_17237	Rückgabe der Selbstauskunft von Software Modulen über Benutzerschnittstelle	gemSpec_OM
A_17792	Rückgabe der Selbstauskunft von Software Modulen auf Dateibasis	gemSpec_OM
GS−A_5034	Inhalte der Betriebsdokumentation der dezentralen Produkte der TI-Plattform	gemSpec_OM

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
A_19899	Fehlermeldungen sind nutzerfreundlich und basieren einheitlich auf UTC	gemSpec_IDP_Dienst
A_19861	Authorization-Endpunkt Authenticator-Modul	gemSpec_IDP_Dienst
A_19863	Schutz vor überalterter Software (Apple)	gemSpec_IDP_Dienst
A_19864	Authenticator im Google Play Store	gemSpec_IDP_Dienst
A_19865	Schutz vor überalterter Software (Android)	gemSpec_IDP_Dienst
A_19853	Protokollierung der Consent-Bestätigung	gemSpec_IDP_Dienst

A_19851	Aufbewahrung alter Schlüssel	gemSpec_IDP_Dienst
A_19838	Verarbeitung des Consent	gemSpec_IDP_Dienst
A_19840	Inhalte des Claims	gemSpec_IDP_Dienst
A_19842	Maximale Gültigkeitsdauer des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19843	Maximale Gültigkeitsdauer des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_20140	Token-Endpunkt (Datensparsamkeit)	gemSpec_IDP_Dienst
A_20141	Token (Identifikation des Nutzers)	gemSpec_IDP_Dienst
A_19828	Annahme und Prüfung des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19816	Verschlüsselung des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19794	Mindestangaben für den Token-Widerruf (Token Revocation minimal information)	gemSpec_IDP_Dienst
A_20131	Nur vollständige Token-Widerrufsanfragen werden bearbeitet	gemSpec_IDP_Dienst
A_19792	Widerruf des "REFRESH_TOKEN" ("refresh_token" Revocation)	gemSpec_IDP_Dienst
A_19791	Widerruf des "ID_TOKEN" ("id_token" Revocation)	gemSpec_IDP_Dienst
A_19788	Widerruf der "SUBJECT_SESSION" durch Authenticator	gemSpec_IDP_Dienst
A_20018	Widerruf der "SUBJECT_SESSION" durch Fachdienste	gemSpec_IDP_Dienst
A_19789	Widerruf der "SUBJECT_SESSION" durch Backchannel Revocation	gemSpec_IDP_Dienst
A_19790	Backchannel Revocation Information an Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19787	Verwendung terminierter "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19784	Rückmeldung des Status-Code der erfolgreichen Widerrufsumsetzung [RFC7009#section-2.2]	gemSpec_IDP_Dienst
A_19783	Rückmeldung des Status-Code der nicht erfolgten Widerrufsumsetzung	gemSpec_IDP_Dienst

A_19782	Informationen am Userinfo-Endpunkt	gemSpec_IDP_Dienst
GS−A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS−A_4368	Schlüsselerzeugung	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_4384	TLS-Verbindungen	gemSpec_Krypt
GS−A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17124	TLS-Verbindungen (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
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_6521	Zulassungstest: TBI	gemKPT_Test
TIP1−A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1−A_4923	Dauerhafte Verfügbarkeit RU und TU	gemKPT_Test
TIP1−A_2724	TBI verantwortet Betrieb RU und TU	gemKPT_Test
TIP1−A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1−A_6527	Testkarten	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_4930	Automatisierung von Tests	gemKPT_Test
TIP1−A_2720	RU/TU: Funktionales Abbild der Produktivumgebung	gemKPT_Test
TIP1−A_2726	Bestandteile RU und TU	gemKPT_Test
TIP1−A_2722−01	TBI integriert die Produkttypen in seine Systemumgebung	gemKPT_Test
TIP1−A_3017	Systemumgebungsmanagement RU sowie TU	gemKPT_Test
TIP1−A_3361	Dokumentation für den Betrieb in der RU und TU bereitstellen	gemKPT_Test
TIP1−A_2738	Exklusiver Zugriff organisatorisch	gemKPT_Test
TIP1−A_7330	Tracedaten von echten Außenschnittstellen	gemKPT_Test
TIP1−A_7331	Bereitstellung von Tracedaten an Außenschnittstelle	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_2775	Performance in RU	gemKPT_Test
TIP1−A_6086	Unterstützung bei Anbindung eines Produktes	gemKPT_Test
TIP1−A_3363	Nutzung von Produkt-Schnittstellen in der TU	gemKPT_Test
TIP1−A_4192	Dimensionierung TU für PU-Fehlernachstellung	gemKPT_Test
TIP1−A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1−A_2806	Zeitnahe Anpassung der Konfiguration der Testumgebung	gemKPT_Test
TIP1−A_2803−01	Nachstellen von PU-Fehlern in der TU	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_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1−A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1−A_6524−01	Testdokumentation gemäß Vorlagen	gemKPT_Test
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_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS−A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
A_17235	Versionierung von Software Modulen durch die Produktidentifikation	gemSpec_OM
GS−A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	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_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM

GS−A_4864	Logging-Vorgaben nach dem Übergang zum Produktivbetrieb	gemSpec_OM

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 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 4: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19870	Verwendung eindeutiger URI	gemSpec_IDP_Dienst
A_19872	Discovery Document interne und externe Adressierung	gemSpec_IDP_Dienst
A_19873	Inhalte des Discovery Documents	gemSpec_IDP_Dienst
A_19899	Fehlermeldungen sind nutzerfreundlich und basieren einheitlich auf UTC	gemSpec_IDP_Dienst
A_19861	Authorization-Endpunkt Authenticator-Modul	gemSpec_IDP_Dienst
A_19862	Authenticator im Apple App Store	gemSpec_IDP_Dienst
A_19863	Schutz vor überalterter Software (Apple)	gemSpec_IDP_Dienst
A_19864	Authenticator im Google Play Store	gemSpec_IDP_Dienst
A_19865	Schutz vor überalterter Software (Android)	gemSpec_IDP_Dienst
A_19850	Enschlüsseln der Eingangsdaten am Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19849	ACCESS_CODE und ID_- oder REFRESH_TOKEN nur für gültige Zertifikate	gemSpec_IDP_Dienst
A_19836	Signaturprüfung des Consent	gemSpec_IDP_Dienst
A_19837	Schematische Prüfung des Consent	gemSpec_IDP_Dienst
A_19839	Der Authorization-Endpunkt bestätigt ausschließlich Zertifikatsinformationen	gemSpec_IDP_Dienst

A_19844	Maximale Gültigkeitsdauer des "ID_TOKEN"	gemSpec_IDP_Dienst
A_19845	Nutzer-Informationen im Claim	gemSpec_IDP_Dienst
A_20140	Token-Endpunkt (Datensparsamkeit)	gemSpec_IDP_Dienst
A_19977	Keine Token für widerrufene Entitäten	gemSpec_IDP_Dienst
A_19978	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_19846	Signatur des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_20107	Redirection-Endpunkt Auswertung HTTP-Header	gemSpec_IDP_Dienst
A_19827	"ID_TOKEN" Protokollierung in allen Fällen	gemSpec_IDP_Dienst
A_19829	"REFRESH_TOKEN" Protokollierung nur im Negativfall	gemSpec_IDP_Dienst
A_19807	Nur Fachdienste führen Token Introspection durch	gemSpec_IDP_Dienst
A_19808	Inhalte der Token Introspection Antwort	gemSpec_IDP_Dienst
A_19794	Mindestangaben für den Token-Widerruf (Token Revocation minimal information)	gemSpec_IDP_Dienst
A_19792	Widerruf des "REFRESH_TOKEN" ("refresh_token" Revocation)	gemSpec_IDP_Dienst
A_19791	Widerruf des "ID_TOKEN" ("id_token" Revocation)	gemSpec_IDP_Dienst
A_19788	Widerruf der "SUBJECT_SESSION" durch Authenticator	gemSpec_IDP_Dienst
A_20018	Widerruf der "SUBJECT_SESSION" durch Fachdienste	gemSpec_IDP_Dienst
A_19789	Widerruf der "SUBJECT_SESSION" durch Backchannel Revocation	gemSpec_IDP_Dienst
A_19790	Backchannel Revocation Information an Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19787	Verwendung terminierter "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19784	Rückmeldung des Status-Code der erfolgreichen Widerrufsumsetzung [RFC7009#section-2.2]	gemSpec_IDP_Dienst
A_19783	Rückmeldung des Status-Code der nicht erfolgten Widerrufsumsetzung	gemSpec_IDP_Dienst

A_19782	Informationen am Userinfo-Endpunkt	gemSpec_IDP_Dienst
A_20057	Token Introspection Response Inhalte	gemSpec_IDP_FD
GS−A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
GS−A_5541	TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM	gemSpec_Krypt
GS−A_5580−01	TLS-Klient für betriebsunterstützende Dienste	gemSpec_Krypt
GS−A_5581	"TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI)	gemSpec_Krypt
GS−A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	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_4944−01	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
GS−A_4945−01	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
GS−A_4946−01	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
GS−A_4947−01	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
A_17178	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
A_17179	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
A_19163	Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes	gemSpec_DS_Hersteller
A_19164	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller

A_19165	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller

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)
A_19881	Gültigkeitsdauer von JSON-Schlüsselmaterial	gemSpec_IDP_Dienst
A_19874	Bereitstellung Internes Discovery Document innerhalb der TI	gemSpec_IDP_Dienst
A_19860	Der Authorization-Endpunkt Standards	gemSpec_IDP_Dienst
A_19788	Widerruf der "SUBJECT_SESSION" durch Authenticator	gemSpec_IDP_Dienst
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt
A_19148	Sicherheits- und Datenschutzkonzept	gemSpec_DS_Hersteller
A_19147	Sicherheitstestplan	gemSpec_DS_Hersteller
A_19150	Umsetzung Sicherheitstestplan	gemSpec_DS_Hersteller
A_19151	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
A_19152	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
A_19153	Sicherheitsrelevanter Softwarearchitektur-Review	gemSpec_DS_Hersteller
A_19154	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
A_19155	Durchführung sicherheitsrelevanter Quellcode-Reviews	gemSpec_DS_Hersteller
A_19156	Durchführung automatisierter Sicherheitstests	gemSpec_DS_Hersteller
A_19157	Dokumentierter Plan zur Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19158	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
A_19159	Dokumentation des sicheren Produktlebenszyklus	gemSpec_DS_Hersteller

A_19160	Änderungs- und Konfigurationsmanagementprozess	gemSpec_DS_Hersteller
A_19161	Verifizierung der Einhaltung sicherheitstechnische Eignung durch Datenschutzbeauftragten	gemSpec_DS_Hersteller
A_19162	Informationspflicht bei Veröffentlichung neue Produktversion	gemSpec_DS_Hersteller

3.2.3 Produktgutachten

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

Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_19875	Absicherung des Internen Discovery Document innerhalb der TI mit TLS	gemSpec_IDP_Dienst
A_19877	Bereitstellung Externes Discovery Document im Internet	gemSpec_IDP_Dienst
A_19880	Bereitstellung der PUK	gemSpec_IDP_Dienst
A_19895	Erweiterte Nutzung von Schlüsseln	gemSpec_IDP_Dienst
A_19896	Format der Fehlermeldungen	gemSpec_IDP_Dienst
A_19894	Dynamische Registrierung (Absicherung durch TLS)	gemSpec_IDP_Dienst
A_20145	Das Discovery Document enthält statische Adressen	gemSpec_IDP_Dienst
A_19909	Integrität der Eingangsdaten am Authenticator-Modul	gemSpec_IDP_Dienst
A_20146	Redirection-Endpunkt (Herausgabe von Informationen an Redirection-Endpunkt)	gemSpec_IDP_Dienst
A_20147	Redirection-Endpunkt (Verantwortlichkeit für Aktualität)	gemSpec_IDP_Dienst
A_20148	Discovery Document (Datenbasis Anwendungsfrontend autoclean)	gemSpec_IDP_Dienst
A_20149	Discovery Document (Datenbasis Authenticator autoclean)	gemSpec_IDP_Dienst

A_20150	Das Discovery Document ist maximal 24 Stunden alt	gemSpec_IDP_Dienst
A_20151	Zusätzlicher Schutz des Discovery Documents	gemSpec_IDP_Dienst
A_19853	Protokollierung der Consent-Bestätigung	gemSpec_IDP_Dienst
A_19850	Enschlüsseln der Eingangsdaten am Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19851	Aufbewahrung alter Schlüssel	gemSpec_IDP_Dienst
A_19852	Verwendung des Attributes "auth_time"	gemSpec_IDP_Dienst
A_19848	Verwendung des Attributes "Bearer"	gemSpec_IDP_Dienst
A_19849	ACCESS_CODE und ID_- oder REFRESH_TOKEN nur für gültige Zertifikate	gemSpec_IDP_Dienst
A_19835	Entschlüsselung des Consent	gemSpec_IDP_Dienst
A_19836	Signaturprüfung des Consent	gemSpec_IDP_Dienst
A_19837	Schematische Prüfung des Consent	gemSpec_IDP_Dienst
A_19838	Verarbeitung des Consent	gemSpec_IDP_Dienst
A_19839	Der Authorization-Endpunkt bestätigt ausschließlich Zertifikatsinformationen	gemSpec_IDP_Dienst
A_19840	Inhalte des Claims	gemSpec_IDP_Dienst
A_19841	Maximale Gültigkeitsdauer einer "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19842	Maximale Gültigkeitsdauer des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19843	Maximale Gültigkeitsdauer des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19844	Maximale Gültigkeitsdauer des "ID_TOKEN"	gemSpec_IDP_Dienst
A_19845	Nutzer-Informationen im Claim	gemSpec_IDP_Dienst
A_19977	Keine Token für widerrufene Entitäten	gemSpec_IDP_Dienst
A_19978	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_19847	Verschlüsselung des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_19832	Sichere Übertragung des "ACCESS_CODE"	gemSpec_IDP_Dienst
A_20106	Bereitstellung Redirection-Endpunkt	gemSpec_IDP_Dienst
A_20110	Absicherung Redirection-Endpunkt	gemSpec_IDP_Dienst

A_20108	Redirection-Endpunkt-Ergänzung mit Portangaben	gemSpec_IDP_Dienst
A_19825	Annahme und Prüfung von "ACCESS_CODE" und "SECRET"	gemSpec_IDP_Dienst
A_19826	"ACCESS_CODE" einmalige Verwendung	gemSpec_IDP_Dienst
A_19820	Erfolgreiche Antwort auf "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19821	Signatur des "ID_TOKEN" und "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19822	Verschlüsselung des "ID_TOKEN"	gemSpec_IDP_Dienst
A_19817	Signatur des "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19818	"REFRESH_TOKEN" mathematische und zeitliche Gültigkeit	gemSpec_IDP_Dienst
A_19819	"REFRESH_TOKEN" Integritätsprüfung	gemSpec_IDP_Dienst
A_19809	Sichere Übertragung von "ID_TOKEN" und "REFRESH_TOKEN"	gemSpec_IDP_Dienst
A_19811	Adressierung der Token beim Versand	gemSpec_IDP_Dienst
A_19812	Token Introspection Timeout	gemSpec_IDP_Dienst
A_19807	Nur Fachdienste führen Token Introspection durch	gemSpec_IDP_Dienst
A_19808	Inhalte der Token Introspection Antwort	gemSpec_IDP_Dienst
A_19799	Die Token Introspection Antwort ist signiert	gemSpec_IDP_Dienst
A_19800	Die Token Introspection Antwort ist verschlüsselt	gemSpec_IDP_Dienst
A_19796	Verwendung von Transport Layer Security (TLS) bei Token Introspection	gemSpec_IDP_Dienst
A_19794	Mindestangaben für den Token-Widerruf (Token Revocation minimal information)	gemSpec_IDP_Dienst
A_19795	Token-Widerrufsanfragen sind zu signieren	gemSpec_IDP_Dienst
A_19792	Widerruf des "REFRESH_TOKEN" ("refresh_token" Revocation)	gemSpec_IDP_Dienst
A_19791	Widerruf des "ID_TOKEN" ("id_token" Revocation)	gemSpec_IDP_Dienst
A_20018	Widerruf der "SUBJECT_SESSION" durch Fachdienste	gemSpec_IDP_Dienst
A_19789	Widerruf der "SUBJECT_SESSION" durch Backchannel Revocation	gemSpec_IDP_Dienst

A_19790	Backchannel Revocation Information an Authorization-Endpunkt	gemSpec_IDP_Dienst
A_19787	Verwendung terminierter "SUBJECT_SESSION"	gemSpec_IDP_Dienst
A_19784	Rückmeldung des Status-Code der erfolgreichen Widerrufsumsetzung [RFC7009#section-2.2]	gemSpec_IDP_Dienst
A_19783	Rückmeldung des Status-Code der nicht erfolgten Widerrufsumsetzung	gemSpec_IDP_Dienst
A_19782	Informationen am Userinfo-Endpunkt	gemSpec_IDP_Dienst
A_19751	Inhalte des Claims für Versicherte (eGK)	gemSpec_IDP_FD
A_19752	Inhalte des Claims für Leistungserbringer (HBA)	gemSpec_IDP_FD
A_19753	Inhalte des Claims für SMC-B	gemSpec_IDP_FD
A_19763	Negative Token Introspection	gemSpec_IDP_FD
GS−A_4357	X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen	gemSpec_Krypt
GS−A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS−A_4361	X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen	gemSpec_Krypt
GS−A_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_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
A_18986	Fachdienst-interne TLS-Verbindungen	gemSpec_Krypt
GS−A_4389	Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt

GS−A_4390	Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten	gemSpec_Krypt
GS−A_5016	Symmetrische Verschlüsselung binärer Daten	gemSpec_Krypt
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt

4 Anhang – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria
ST	Security Target

4.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion 6
Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"..... 7
Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung" 14
Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung".....19
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ...22
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten".....23

4.3 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
[gemZul_Prod_Frontend_Vers_ePA]	gematik: Verfahrensbeschreibung Zulassung Produkte der Telematikinfrastruktur hier: ePA-Frontend des Versicherten