Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Identity Provider - Dienst

Produkttyp Version:	2.2.0-0
Produkttyp Status:	freigegeben

Version:	1.0.0
Revision:	374627
Stand:	14.06.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_IDP-Dienst_PTV_2.2.0-0

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.

Für die Produkttypversion 2.2.0-0 sind entsprechende Teile aus den Feature-Spezifikationen gemF_Tokenverschlüsselung und gemF_Biometrie sowie aus der Änderungsliste IdP_Maintenance_21.1 Grundlage für die Änderungen.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0-0	Initiale Version auf Dokumentenebene	gemProdT_IDP-Dienst_PTV_1.0.0-0
2.0.0-0	Anpassung auf Releasestand 4.0.1	gemProdT_IDP-Dienst_PTV_2.0.0-0
2.1.0-0	Anpassung auf Releasestand 4.0.1 Hotfix 1	gemProdT_IDP-Dienst_PTV_2.1.0-0
2.2.0-0	Anpassung auf Releasestand IDP 2.2.0 (inkl. entsprechender Anteile aus gemF_Tokenverschlüsselung & gemF_Biometrie) und der Änderungsliste IdP_Maintenance_21.1	gemProdT_IDP-Dienst_PTV_2.2.0-0

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	14.06.21		freigegeben	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 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 Identity Provider Dienstes (IDP-Dienst) 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. gemPTV_ATV_Festlegungen, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

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

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können 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
gemKPT_Test	Testkonzept der TI	2.~~7~~8.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.14.0
gemSpec_SST_LD_BD	Spezifikation Logdaten und Betriebsdatenerfassung	1.2.0
gemSpec_IDP_Frontend	Spezifikation Identity Provider - Frontend	1.~~1~~2.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.1~~8~~9.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.1~~2~~3.0
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.3.0
gemSpec_IDP_Dienst	Spezifikation Identity Provider - Dienst	1.~~1~~3.~~1~~0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.10.~~1~~2
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.~~19.~~20.1

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)
A_20313	Inhalte des Claims	gemSpec_IDP_Dienst
A_20314-01	Maximale Gültigkeitsdauer des "AUTHORIZATION_CODE" und des "CHALLENGE_TOKEN"	gemSpec_IDP_Dienst
A_20315-01	"AUTHORIZATION_CODE" nach Gültigkeitsende nicht mehr verwenden	gemSpec_IDP_Dienst
A_20318	Keine Token für widerrufene Entitäten	gemSpec_IDP_Dienst
A_20321-01	Annahme und Prüfung von "AUTHORIZATION_CODE" und "KEY_VERIFIER"	gemSpec_IDP_Dienst
A_20323	TOKEN-Ausgabe Protokollierung in allen Fällen	gemSpec_IDP_Dienst
A_20327-02	Signatur des "ID_TOKEN" und "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20330	Ausgabe der Token	gemSpec_IDP_Dienst
A_20376	Verwendung des Attributes "state"	gemSpec_IDP_Dienst
A_20377	Verwendung des Attributes "state"	gemSpec_IDP_Dienst
A_20434	Einhaltung der Standards bei der Realisierung des Authorization-Endpunkts	gemSpec_IDP_Dienst
A_20439	Das Discovery Document enthält statische Adressen	gemSpec_IDP_Dienst
A_20440-01	Schematische Prüfung des Consent	gemSpec_IDP_Dienst
A_20458-02	Inhalte des Discovery Document	gemSpec_IDP_Dienst
A_20459	Das Attribut AUTH_TIME muss in allen Token unverändert bleiben	gemSpec_IDP_Dienst
A_20462	Maximale Gültigkeitsdauer des "ID_TOKEN"	gemSpec_IDP_Dienst
A_20463	Maximale Gültigkeitsdauer des "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20464	Token-Endpunkt (Datensparsamkeit)	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20465	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_20521-02	Inhalt des CHALLENGE_TOKEN an das Authenticator-Modul	gemSpec_IDP_Dienst
A_20522	Erstellen einer "SESSION_ID"	gemSpec_IDP_Dienst
A_20523	Zusammenstellung der Claims zum "user_consent"	gemSpec_IDP_Dienst
A_20524-02	Befüllen der Claims "given_name", "family_name", "organizationName", "professionOID", "idNummer", "acr" und "amr"	gemSpec_IDP_Dienst
A_20588-01	IdP-Dienst - Erkennung Clientsystem User-Agent	gemSpec_IDP_Dienst
A_20589	IdP-Dienst – Ausschluss bestimmter Clientsystem-Versionsnummern von der Kommunikation	gemSpec_IDP_Dienst
A_20591-01	Festlegungen zur Signatur der Discovery Documents	gemSpec_IDP_Dienst
A_20687-01	Bereitstellung der öffentlichen Schlüsselteile	gemSpec_IDP_Dienst
A_20688	Discovery Document interne und externe Adressierung	gemSpec_IDP_Dienst
A_20691-01	Das Discovery Document ist maximal 24 Stunden alt	gemSpec_IDP_Dienst
A_20692-01	Maximale Gültigkeitsdauer eines SSO_TOKEN	gemSpec_IDP_Dienst
A_20693-01	Senden des "AUTHORIZATION_CODE" und "SSO_TOKEN" an die "REDIRECT_URI"	gemSpec_IDP_Dienst
A_20694	Zusammenstellung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20695-01	Signieren des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20696	Verschlüsselung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20697	Zusammenstellung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20698	Annahme des Authorization Request	gemSpec_IDP_Dienst
A_20699-03	Annahme von CHALLENGE_TOKEN: Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_20731	Verwendung des Attributes "auth_time"	gemSpec_IDP_Dienst
A_20732	Aufnahme der öffentlichen Schlüssel in das Discovery Document	gemSpec_IDP_Dienst
A_20946-01	Annahme eines "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20947	Entschlüsselung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20948-01	Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20949	Anforderung einer Authentisierung bei negativer Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20950-01	Positive Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20951-01	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
A_20952	Claim "aud" im Token setzen	gemSpec_IDP_Dienst
A_21315-01	Bereitstellung einer URI zum Einreichen von SSO_TOKEN	gemSpec_IDP_Dienst
A_21317	Verschlüsselung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_21318	Prüfung des "AUTHORIZATION_CODE“	gemSpec_IDP_Dienst
A_21319	Prüfung des "CODE_VERIFIER"	gemSpec_IDP_Dienst
A_21320	Entschlüsseln des "Token-Key"	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21321	Verschlüsselung von "ACCESS_TOKEN" und "ID_TOKEN"	gemSpec_IDP_Dienst
A_21330	Ablaufzeitpunkt von "AUTHORIZATION_CODE" und "SSO_TOKEN"	gemSpec_IDP_Dienst
A_21411	Registrierungsfunktion des IdP-Dienstes: Fehlermeldungen	gemSpec_IDP_Dienst
A_21412	Registrierungsfunktion des IdP-Dienstes: Registrierung	gemSpec_IDP_Dienst
A_21413	Registrierungsfunktion des IdP-Dienstes: Prüfung des Scope	gemSpec_IDP_Dienst
A_21415	Registrierungsfunktion des IdP-Dienstes: Datenformate und Syntax zur Kommunikation mit dem Authenticator-Modul	gemSpec_IDP_Dienst
A_21419	Registrierungsfunktion des IdP-Dienstes: Anforderung an die Authentifizierung des Nutzers	gemSpec_IDP_Dienst
A_21420	Registrierungsfunktion des IdP-Dienstes: Entschlüsselung der Registrierungsdaten	gemSpec_IDP_Dienst
A_21421	Registrierungsfunktion des IdP-Dienstes: Validierung der signierten Pairing-Daten	gemSpec_IDP_Dienst
A_21422	Registrierungsfunktion des IdP-Dienstes: Validierung des Zusammenhangs von ACCESS_TOKEN und Pairing-Daten	gemSpec_IDP_Dienst
A_21423	Registrierungsfunktion des IdP-Dienstes: Bewertung des Gerätetyps	gemSpec_IDP_Dienst
A_21424	Registrierungsfunktion des IdP-Dienstes: Speicherung der Pairing-Daten	gemSpec_IDP_Dienst
A_21425	Registrierungsfunktion des IdP-Dienstes: Validierung des übermittelten ACCESS_TOKENS	gemSpec_IDP_Dienst
A_21427	Registrierungsfunktion des IdP-Dienstes: Rückmeldung an den Nutzer	gemSpec_IDP_Dienst
A_21428	Erweiterung des Authorization-Endpunkts: Fehlermeldungen	gemSpec_IDP_Dienst
A_21429-02	Erweiterung des Authorization-Endpunkts: Realisierung verschiedener Authentifizierungsmethoden	gemSpec_IDP_Dienst
A_21432	Erweiterung des Authorization-Endpunkts: Prüfung der vorliegenden Gerätedaten	gemSpec_IDP_Dienst
A_21433	Erweiterung des Authorization-Endpunkts: Validierung des Authentifizierungszertifikats	gemSpec_IDP_Dienst
A_21434	Erweiterung des Authorization-Endpunkts: Auslesen der gespeicherten Pairing-Daten	gemSpec_IDP_Dienst
A_21435	Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der gespeicherten Pairing-Daten	gemSpec_IDP_Dienst
A_21437	Erweiterung des Authorization-Endpunkts: Bewertung der Gültigkeit des öffentlichen Schlüssels in den Pairing-Daten	gemSpec_IDP_Dienst
A_21438	Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der signierten Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_21439	Erweiterung des Authorization-Endpunkts: Zu unterstützende Algorithmen zur Prüfung der mathematischen Integrität der signierten Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_21440	Erweiterung des Authorization-Endpunkts: Produktion des Authorization Code und eines SSO_TOKEN	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21441	Inspektions- und Deregistrierungsfunktion des IDP-Dienstes: Fehlermeldungen	gemSpec_IDP_Dienst
A_21445	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des ACCESS_TOKEN	gemSpec_IDP_Dienst
A_21447	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Annahme des Kommandos zur Deaktivierung des Pairings	gemSpec_IDP_Dienst
A_21448	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Deaktivierung des identifizierten Pairing-Datensatzes	gemSpec_IDP_Dienst
A_21449	Erweiterung des Authorization-Endpunkts: Datenmodell und Syntax zur Kommunikation mit dem Authenticator-Modul	gemSpec_IDP_Dienst
A_21450	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Datenmodell und Syntax zur Kommunikation mit dem Authenticator-Modul	gemSpec_IDP_Dienst
A_21452	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Rückgabe der Pairing-Daten	gemSpec_IDP_Dienst
A_21470	Registrierungsfunktion des IdP-Dienstes: Prüfung des Zusammenhangs zwischen Pairing-Daten und übermittelten Authentifizierungszertifikat	gemSpec_IDP_Dienst
A_21472	SSO_TOKEN nur für Mobile Endgeräte und nicht für Primärsysteme	gemSpec_IDP_Dienst
A_21442	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Authentisierung des Nutzers	gemSpec_IDP_Frontend
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_21332	E-Rezept: TLS-Vorgaben	gemSpec_Krypt
GS-A_4359	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS-A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
A_17700	TSL-Auswertung ServiceTypeIdentifier "unspecified"	gemSpec_PKI
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4646	TUC_PKI_017: Lokalisierung TSL Download-Adressen	gemSpec_PKI
GS-A_4647	TUC_PKI_016: Download der TSL-Datei	gemSpec_PKI
GS-A_4648	TUC_PKI_019: Prüfung der Aktualität der TSL	gemSpec_PKI
GS-A_4649	TUC_PKI_020: XML-Dokument validieren	gemSpec_PKI
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	gemSpec_PKI
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	gemSpec_PKI
GS-A_4652-01	TUC_PKI_018: Zertifikatsprüfung in der TI	gemSpec_PKI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4653-01	TUC_PKI_002: Gültigkeitsprüfung des Zertifikats	gemSpec_PKI
GS-A_4654-01	TUC_PKI_003: CA-Zertifikat finden	gemSpec_PKI
GS-A_4655-01	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	gemSpec_PKI
GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	gemSpec_PKI
GS-A_4657-03	TUC_PKI_006: OCSP-Abfrage	gemSpec_PKI
GS-A_4660-02	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS-A_4661-01	kritische Erweiterungen in Zertifikaten	gemSpec_PKI
GS-A_4662	Bedingungen für TLS-Handshake	gemSpec_PKI
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	gemSpec_PKI
GS-A_4749-01	TUC_PKI_007: Prüfung Zertifikatstyp	gemSpec_PKI
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	gemSpec_PKI
GS-A_4829	TUCs, Fehlerbehandlung	gemSpec_PKI
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4943	Alter der OCSP-Responses für eGK-Zertifikate	gemSpec_PKI
GS-A_4957-01	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
GS-A_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	gemSpec_PKI
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_17755	Performance - Rohdaten-Performance-Berichte - Name der Berichte	gemSpec_Perf
A_17756	Performance - Rohdaten-Performance-Berichte - Korrektheit	gemSpec_Perf
A_17757-01	Performance - Rohdaten-Performance-Lieferung - zu liefernde Dateien	gemSpec_Perf
A_19717-02	Performance – IdP-Dienst – Bearbeitungszeit unter Last	gemSpec_Perf
A_20242-01	Performance - Rohdaten-Performance-Berichte - Format der Einträge des Performance-Berichts IdP-Dienst	gemSpec_Perf
A_20243	Performance - IdP-Dienst - Robustheit gegenüber Lastspitzen	gemSpec_Perf
A_20245-02	Performance - Messpunkte für die Erfassung von Rohdaten am IdP-Dienst	gemSpec_Perf
A_20246-01	Performance - Erfassung von Rohdaten bei fehlerhaften Operationen - IdP-Dienst	gemSpec_Perf
A_20247	Performance - Erfassung von Rohdaten - IdP-Dienst	gemSpec_Perf
A_21340	IDP- Abbruch bei OCSP-Timeout	gemSpec_Perf
A_17416-01	Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste	gemSpec_SST_LD_BD

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17733-01	Schnittstelle Betriebsdatenerfassung Datei-Upload	gemSpec_SST_LD_BD
~~A_19863~~	~~Schutz vor überalterter Software (Apple)~~	~~gemSpec_IDP_Dienst~~
~~A_19865~~	~~Schutz vor überalterter Software (Android)~~	~~gemSpec_IDP_Dienst~~
~~A_19874-03~~	~~Bereitstellung des internen Discovery Documents innerhalb der TI~~	~~gemSpec_IDP_Dienst~~
~~A_19877-01~~	~~Bereitstellung des externen Discovery Documents im Internet~~	~~gemSpec_IDP_Dienst~~
~~A_20310~~	~~Verarbeitung des Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20314~~	~~Maximale Gültigkeitsdauer des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20315~~	~~"AUTHORIZATION_CODE" nach Gültigkeitsende nicht mehr verwenden~~	~~gemSpec_IDP_Dienst~~
~~A_20319~~	~~Signatur des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20320~~	~~Sichere Übertragung des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20321~~	~~Annahme und Prüfung von "AUTHORIZATION_CODE" und "CODE_VERIFIER"~~	~~gemSpec_IDP_Dienst~~
~~A_20327~~	~~Signatur des "ID_TOKEN", "ACCESS_TOKEN" und "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20328~~	~~Verschlüsselung des "ACCESS_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20329~~	~~Sichere Übertragung von "ID_TOKEN", "ACCESS_TOKEN" und "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20379~~	~~Abbruch bei schematischer Inkonsistenz im Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20440~~	~~Schematische Prüfung des Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20457~~	~~Verwendung eindeutiger URI~~	~~gemSpec_IDP_Dienst~~
~~A_20458~~	~~Inhalte des Discovery Documents~~	~~gemSpec_IDP_Dienst~~
~~A_20460~~	~~Der Authorization-Endpunkt bestätigt ausschließlich Zertifikatsinformationen~~	~~gemSpec_IDP_Dienst~~
~~A_20474~~	~~"AUTHORIZATION_CODE" einmalige Verwendung~~	~~gemSpec_IDP_Dienst~~
~~A_20521-01~~	~~Inhalt der Challenge an das Authenticator-Modul~~	~~gemSpec_IDP_Dienst~~
~~A_20524~~	~~Befüllen der Claims "given_name", "family_name", "organizationName", "professionOID" und "idNummer"~~	~~gemSpec_IDP_Dienst~~
~~A_20586-01~~	~~IdP-Dienst - Verhalten bei Vollauslastung~~	~~gemSpec_IDP_Dienst~~
~~A_20588~~	~~IdP-Dienst - Erkennung Clientsystem User-Agent~~	~~gemSpec_IDP_Dienst~~
~~A_20591~~	~~Festlegungen zur Signatur der Discovery Documents~~	~~gemSpec_IDP_Dienst~~
~~A_20604~~	~~Signatur der Challenge~~	~~gemSpec_IDP_Dienst~~
~~A_20686~~	~~Erweiterte Nutzung von Schlüsseln~~	~~gemSpec_IDP_Dienst~~
~~A_20687~~	~~Bereitstellung der PUK~~	~~gemSpec_IDP_Dienst~~
~~A_20689~~	~~Internes Discovery Document - Prüfung vor Veröffentlichung~~	~~gemSpec_IDP_Dienst~~
~~A_20690~~	~~Externes Discovery Document - Prüfung vor Veröffentlichung~~	~~gemSpec_IDP_Dienst~~
~~A_20691~~	~~Das Discovery Document ist maximal 24 Stunden alt~~	~~gemSpec_IDP_Dienst~~
~~A_20692~~	~~Maximale Gültigkeitsdauer einer "SUBJECT_SESSION"~~	~~gemSpec_IDP_Dienst~~
~~A_20693~~	~~Senden des "AUTHORIZATION_CODE" und "SSO_TOKEN" an die "REDIRECT_URI"~~	~~gemSpec_IDP_Dienst~~

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20695~~	~~Signieren des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20699~~	~~Annahme der signierten "CHALLENGE"~~	~~gemSpec_IDP_Dienst~~
~~A_20742~~	~~Vergabe der "client_id" durch den IdP-Dienst~~	~~gemSpec_IDP_Dienst~~
~~A_20946~~	~~Annahme eines "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20948~~	~~Validierung des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20950~~	~~Positive Validierung des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20951~~	~~Validierung der Signatur und des Zertifikats der "CHALLENGE"~~	~~gemSpec_IDP_Dienst~~
~~A_19908-01~~	~~Authenticator-Modul: Prüfung der Signatur des "CHALLENGE_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20068-01~~	~~Authenticator-Modul: Prüfung Internet-Zertifikate~~	~~gemSpec_IDP_Frontend~~
~~A_20284~~	~~Authenticator-Modul: Annahme von "SSO_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20499~~	~~Authenticator-Modul: Temporäre Speicherung von "SSO_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20525~~	~~Authenticator-Modul: Anzeige des "user_consent" und PIN-Abfrage~~	~~gemSpec_IDP_Frontend~~
~~A_20526~~	~~Authenticator-Modul: Response auf die "CHALLENGE" des Authorization-Endpunktes~~	~~gemSpec_IDP_Frontend~~
~~A_20527~~	~~Authenticator-Modul: Übertragung des "AUTHORIZATION_CODE" an das Anwendungsfrontend~~	~~gemSpec_IDP_Frontend~~
~~A_20600~~	~~Authenticator-Modul: Annahme des "user_consent" und des "CHALLENGE_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20601~~	~~Authenticator-Modul: Übergabe des Authorization-Request an den Authorization-Endpunkt~~	~~gemSpec_IDP_Frontend~~
~~A_20607~~	~~Authenticator-Modul: Kommunikation über TLS-Verbindung~~	~~gemSpec_IDP_Frontend~~
~~A_20609~~	~~Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen~~	~~gemSpec_IDP_Frontend~~
~~A_20610~~	~~Authenticator-Modul: HTTP-Header user-agent~~	~~gemSpec_IDP_Frontend~~
~~A_20612~~	~~Authenticator-Modul: Anzeige bei Ablehnung des Authenticator-Moduls~~	~~gemSpec_IDP_Frontend~~
~~A_20613~~	~~Authenticator-Modul: Regelmäßiges Einlesen des Discovery Document~~	~~gemSpec_IDP_Frontend~~
~~A_20614~~	~~Authenticator-Modul: Prüfung der Signatur des Discovery Document~~	~~gemSpec_IDP_Frontend~~
~~A_20617-01~~	~~Authenticator-Modul: Verpflichtende Zertifikatsprüfung~~	~~gemSpec_IDP_Frontend~~
~~A_20618~~	~~Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen~~	~~gemSpec_IDP_Frontend~~
~~A_20700-04~~	~~Authenticator-Modul: Signatur der "CHALLENGE"~~	~~gemSpec_IDP_Frontend~~
~~A_20743~~	~~Prüfung der Aktualität der Komponenten-CA-Zertifikate~~	~~gemSpec_IDP_Frontend~~
~~A_20917~~	~~Prüfung auf Vorhandensein und Verwenden eines gültigen "SSO_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_17237~~	~~Rückgabe der Selbstauskunft von Software-Modulen über Benutzerschnittstelle~~	~~gemSpec_OM~~
~~A_17792~~	~~Rückgabe der Selbstauskunft von Software-Modulen auf Dateibasis~~	~~gemSpec_OM~~

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~GS-A_5034~~	~~Inhalte der Betriebsdokumentation der dezentralen Produkte der TI-Plattform~~	~~gemSpec_OM~~
~~A_17758~~	~~Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung~~	~~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_20242~~	~~Performance - Rohdaten-Performance-Berichte - Format der Einträge des Performance-Berichts IdP-Dienst~~	~~gemSpec_Perf~~
~~A_20245-01~~	~~Performance - Messpunkte für die Erfassung von Rohdaten am IdP-Dienst~~	~~gemSpec_Perf~~
~~A_20246~~	~~Performance - Erfassung von Rohdaten bei fehlerhaften Operationen - IdP-Dienst~~	~~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_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2720	RU/TU: Funktionales Abbild der Produktivumgebung	gemKPT_Test
TIP1-A_2722-01	TBI integriert die Produkttypen in seine Systemumgebung	gemKPT_Test
TIP1-A_2724	TBI verantwortet Betrieb RU und TU	gemKPT_Test
TIP1-A_2726	Bestandteile RU und TU	gemKPT_Test
TIP1-A_2738	Exklusiver Zugriff organisatorisch	gemKPT_Test
TIP1-A_2775	Performance in RU	gemKPT_Test
TIP1-A_2803-01	Nachstellen von PU-Fehlern in der TU	gemKPT_Test
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test
TIP1-A_2806	Zeitnahe Anpassung der Konfiguration der Testumgebung	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_3363	Nutzung von Produkt-Schnittstellen in der TU	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_4192	Dimensionierung TU für PU-Fehlernachstellung	gemKPT_Test
TIP1-A_4923	Dauerhafte Verfügbarkeit RU und TU	gemKPT_Test
TIP1-A_4930	Automatisierung von Tests	gemKPT_Test

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6086	Unterstützung bei Anbindung eines Produktes	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6517-01	Eigenverantwortlicher Test: TBI	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6521	Zulassungstest: TBI	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524-01	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6527	Testkarten	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	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_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_7330	Tracedaten von echten Außenschnittstellen	gemKPT_Test
TIP1-A_7331	Bereitstellung von Tracedaten an Außenschnittstelle	gemKPT_Test
TIP1-A_7333	Parallelbetrieb von Release oder Produkttypversion	gemKPT_Test
TIP1-A_7334	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1-A_7358	Qualität des Produktmusters	gemKPT_Test
A_19874-05	Bereitstellung des internen Discovery Documents innerhalb der TI	gemSpec_IDP_Dienst
A_19877-03	Bereitstellung des externen Discovery Documents im Internet	gemSpec_IDP_Dienst
A_20319-01	Signatur des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20320-01	Sichere Übertragung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20329-01	Sichere Übertragung von "ID_TOKEN" und "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20457	Verwendung eindeutiger URI	gemSpec_IDP_Dienst
A_20680	Format der Fehlermeldungen	gemSpec_IDP_Dienst
A_20681	Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20682-01	Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen	gemSpec_IDP_Dienst
A_20683	Formulierung der Fehlermeldungen	gemSpec_IDP_Dienst
A_20684	Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen	gemSpec_IDP_Dienst
A_20685	Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens	gemSpec_IDP_Dienst
A_20686	Erweiterte Nutzung von Schlüsseln	gemSpec_IDP_Dienst
A_21404	Bewertung von Typen mobiler Endgeräte durch den IdP-Dienst	gemSpec_IDP_Dienst
A_21406	Anforderungen an Transaktionalität der Freischaltung der Einstufung von Gerätetypen	gemSpec_IDP_Dienst
A_21407	Vorhalten von Backup-Daten zur Einstufung von Gerätetypen	gemSpec_IDP_Dienst
A_21410	Registrierung des Pairing-Endpunkts und des Authenticator-Moduls am IdP-Dienst	gemSpec_IDP_Dienst
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4831	Standards für IPv4	gemSpec_Net
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM
GS-A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS-A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS-A_4864	Logging-Vorgaben nach dem Übergang zum Produktivbetrieb	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_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
A_17758	Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung	gemSpec_Perf
A_19718-01	Performance – IdP-Dienst – Verfügbarkeit	gemSpec_Perf
~~A_19863~~	~~Schutz vor überalterter Software (Apple)~~	~~gemSpec_IDP_Dienst~~
~~A_19865~~	~~Schutz vor überalterter Software (Android)~~	~~gemSpec_IDP_Dienst~~
~~A_20592~~	~~Aktualisierung der Discovery Documents~~	~~gemSpec_IDP_Dienst~~
~~A_20682~~	~~Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen~~	~~gemSpec_IDP_Dienst~~
~~A_17235~~	~~Versionierung von Software-Modulen durch die Produktidentifikation~~	~~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_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
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_19874-05	Bereitstellung des internen Discovery Documents innerhalb der TI	gemSpec_IDP_Dienst
A_19877-03	Bereitstellung des externen Discovery Documents im Internet	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20319-01	Signatur des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20320-01	Sichere Übertragung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20329-01	Sichere Übertragung von "ID_TOKEN" und "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20680	Format der Fehlermeldungen	gemSpec_IDP_Dienst
A_20681	Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen	gemSpec_IDP_Dienst
A_20682-01	Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen	gemSpec_IDP_Dienst
A_20683	Formulierung der Fehlermeldungen	gemSpec_IDP_Dienst
A_20684	Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen	gemSpec_IDP_Dienst
A_20685	Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens	gemSpec_IDP_Dienst
A_20688	Discovery Document interne und externe Adressierung	gemSpec_IDP_Dienst
A_21404	Bewertung von Typen mobiler Endgeräte durch den IdP-Dienst	gemSpec_IDP_Dienst
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
GS-A_4362	X.509-Identitäten für Verschlüsselungszertifikate	gemSpec_Krypt
GS-A_5541	TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM	gemSpec_Krypt
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_5580-01	TLS-Klient für betriebsunterstützende Dienste	gemSpec_Krypt
GS-A_5581	"TUC vereinfachte Zertifikatsprüfung“ (Komponenten-PKI)	gemSpec_Krypt
~~A_19863~~	~~Schutz vor überalterter Software (Apple)~~	~~gemSpec_IDP_Dienst~~
~~A_19865~~	~~Schutz vor überalterter Software (Android)~~	~~gemSpec_IDP_Dienst~~
~~A_20592~~	~~Aktualisierung der Discovery Documents~~	~~gemSpec_IDP_Dienst~~
~~A_20682~~	~~Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen~~	~~gemSpec_IDP_Dienst~~

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_19147	Sicherheitstestplan	gemSpec_DS_Hersteller
A_19148	Sicherheits- und Datenschutzkonzept	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
A_21309	Prüfung der Verwendung des Authorization Codes	gemSpec_IDP_Dienst
~~A_19874-03~~	~~Bereitstellung des internen Discovery Documents innerhalb der TI~~	~~gemSpec_IDP_Dienst~~
~~A_17207~~	~~Signaturen binärer Daten (ECC-Migration)~~	~~gemSpec_Krypt~~

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_20313	Inhalte des Claims	gemSpec_IDP_Dienst
A_20314-01	Maximale Gültigkeitsdauer des "AUTHORIZATION_CODE" und des "CHALLENGE_TOKEN"	gemSpec_IDP_Dienst
A_20315-01	"AUTHORIZATION_CODE" nach Gültigkeitsende nicht mehr verwenden	gemSpec_IDP_Dienst
A_20318	Keine Token für widerrufene Entitäten	gemSpec_IDP_Dienst
A_20323	TOKEN-Ausgabe Protokollierung in allen Fällen	gemSpec_IDP_Dienst
A_20327-02	Signatur des "ID_TOKEN" und "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20330	Ausgabe der Token	gemSpec_IDP_Dienst
A_20434	Einhaltung der Standards bei der Realisierung des Authorization-Endpunkts	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_20440-01	Schematische Prüfung des Consent	gemSpec_IDP_Dienst
A_20458-02	Inhalte des Discovery Document	gemSpec_IDP_Dienst
A_20459	Das Attribut AUTH_TIME muss in allen Token unverändert bleiben	gemSpec_IDP_Dienst
A_20462	Maximale Gültigkeitsdauer des "ID_TOKEN"	gemSpec_IDP_Dienst
A_20463	Maximale Gültigkeitsdauer des "ACCESS_TOKEN"	gemSpec_IDP_Dienst
A_20464	Token-Endpunkt (Datensparsamkeit)	gemSpec_IDP_Dienst
A_20465	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_20521-02	Inhalt des CHALLENGE_TOKEN an das Authenticator-Modul	gemSpec_IDP_Dienst
A_20522	Erstellen einer "SESSION_ID"	gemSpec_IDP_Dienst
A_20582-01	IdP-Dienst - Berücksichtigung OWASP-Top-10-Risiken	gemSpec_IDP_Dienst
A_20591-01	Festlegungen zur Signatur der Discovery Documents	gemSpec_IDP_Dienst
A_20691-01	Das Discovery Document ist maximal 24 Stunden alt	gemSpec_IDP_Dienst
A_20692-01	Maximale Gültigkeitsdauer eines SSO_TOKEN	gemSpec_IDP_Dienst
A_20693-01	Senden des "AUTHORIZATION_CODE" und "SSO_TOKEN" an die "REDIRECT_URI"	gemSpec_IDP_Dienst
A_20695-01	Signieren des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20696	Verschlüsselung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20697	Zusammenstellung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_20731	Verwendung des Attributes "auth_time"	gemSpec_IDP_Dienst
A_20946-01	Annahme eines "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20947	Entschlüsselung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20948-01	Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20949	Anforderung einer Authentisierung bei negativer Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20950-01	Positive Validierung des "SSO_TOKEN"	gemSpec_IDP_Dienst
A_20951-01	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
A_21317	Verschlüsselung des "AUTHORIZATION_CODE"	gemSpec_IDP_Dienst
A_21318	Prüfung des "AUTHORIZATION_CODE“	gemSpec_IDP_Dienst
A_21319	Prüfung des "CODE_VERIFIER"	gemSpec_IDP_Dienst
A_21321	Verschlüsselung von "ACCESS_TOKEN" und "ID_TOKEN"	gemSpec_IDP_Dienst
A_21413	Registrierungsfunktion des IdP-Dienstes: Prüfung des Scope	gemSpec_IDP_Dienst
A_21419	Registrierungsfunktion des IdP-Dienstes: Anforderung an die Authentifizierung des Nutzers	gemSpec_IDP_Dienst
A_21420	Registrierungsfunktion des IdP-Dienstes: Entschlüsselung der Registrierungsdaten	gemSpec_IDP_Dienst
A_21421	Registrierungsfunktion des IdP-Dienstes: Validierung der signierten Pairing-Daten	gemSpec_IDP_Dienst
A_21422	Registrierungsfunktion des IdP-Dienstes: Validierung des Zusammenhangs von ACCESS_TOKEN und Pairing-Daten	gemSpec_IDP_Dienst

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21423	Registrierungsfunktion des IdP-Dienstes: Bewertung des Gerätetyps	gemSpec_IDP_Dienst
A_21424	Registrierungsfunktion des IdP-Dienstes: Speicherung der Pairing-Daten	gemSpec_IDP_Dienst
A_21425	Registrierungsfunktion des IdP-Dienstes: Validierung des übermittelten ACCESS_TOKENS	gemSpec_IDP_Dienst
A_21426	Registrierungsfunktion des IdP-Dienstes: Nicht-Speicherung des übermittelten Authentifizierungszertifikats	gemSpec_IDP_Dienst
A_21432	Erweiterung des Authorization-Endpunkts: Prüfung der vorliegenden Gerätedaten	gemSpec_IDP_Dienst
A_21433	Erweiterung des Authorization-Endpunkts: Validierung des Authentifizierungszertifikats	gemSpec_IDP_Dienst
A_21434	Erweiterung des Authorization-Endpunkts: Auslesen der gespeicherten Pairing-Daten	gemSpec_IDP_Dienst
A_21435	Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der gespeicherten Pairing-Daten	gemSpec_IDP_Dienst
A_21437	Erweiterung des Authorization-Endpunkts: Bewertung der Gültigkeit des öffentlichen Schlüssels in den Pairing-Daten	gemSpec_IDP_Dienst
A_21438	Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der signierten Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_21439	Erweiterung des Authorization-Endpunkts: Zu unterstützende Algorithmen zur Prüfung der mathematischen Integrität der signierten Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_21440	Erweiterung des Authorization-Endpunkts: Produktion des Authorization Code und eines SSO_TOKEN	gemSpec_IDP_Dienst
A_21445	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des ACCESS_TOKEN	gemSpec_IDP_Dienst
A_21447	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Annahme des Kommandos zur Deaktivierung des Pairings	gemSpec_IDP_Dienst
A_21448	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Deaktivierung des identifizierten Pairing-Datensatzes	gemSpec_IDP_Dienst
A_21452	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Rückgabe der Pairing-Daten	gemSpec_IDP_Dienst
A_21470	Registrierungsfunktion des IdP-Dienstes: Prüfung des Zusammenhangs zwischen Pairing-Daten und übermittelten Authentifizierungszertifikat	gemSpec_IDP_Dienst
A_21442	Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Authentisierung des Nutzers	gemSpec_IDP_Frontend
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17207	Signaturen binärer Daten (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18986	Fachdienst-interne TLS-Verbindungen	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_21332	E-Rezept: TLS-Vorgaben	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_4384	TLS-Verbindungen	gemSpec_Krypt
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_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
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
~~A_19877-01~~	~~Bereitstellung des externen Discovery Documents im Internet~~	~~gemSpec_IDP_Dienst~~
~~A_20310~~	~~Verarbeitung des Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20314~~	~~Maximale Gültigkeitsdauer des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20315~~	~~"AUTHORIZATION_CODE" nach Gültigkeitsende nicht mehr verwenden~~	~~gemSpec_IDP_Dienst~~
~~A_20319~~	~~Signatur des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20320~~	~~Sichere Übertragung des "AUTHORIZATION_CODE"~~	~~gemSpec_IDP_Dienst~~
~~A_20321~~	~~Annahme und Prüfung von "AUTHORIZATION_CODE" und "CODE_VERIFIER"~~	~~gemSpec_IDP_Dienst~~
~~A_20327~~	~~Signatur des "ID_TOKEN", "ACCESS_TOKEN" und "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20328~~	~~Verschlüsselung des "ACCESS_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20329~~	~~Sichere Übertragung von "ID_TOKEN", "ACCESS_TOKEN" und "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20376~~	~~Verwendung des Attributes "state"~~	~~gemSpec_IDP_Dienst~~
~~A_20377~~	~~Verwendung des Attributes "state"~~	~~gemSpec_IDP_Dienst~~
~~A_20379~~	~~Abbruch bei schematischer Inkonsistenz im Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20439~~	~~Das Discovery Document enthält statische Adressen~~	~~gemSpec_IDP_Dienst~~
~~A_20440~~	~~Schematische Prüfung des Consent~~	~~gemSpec_IDP_Dienst~~
~~A_20457~~	~~Verwendung eindeutiger URI~~	~~gemSpec_IDP_Dienst~~
~~A_20458~~	~~Inhalte des Discovery Documents~~	~~gemSpec_IDP_Dienst~~

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20460~~	~~Der Authorization-Endpunkt bestätigt ausschließlich Zertifikatsinformationen~~	~~gemSpec_IDP_Dienst~~
~~A_20474~~	~~"AUTHORIZATION_CODE" einmalige Verwendung~~	~~gemSpec_IDP_Dienst~~
~~A_20521-01~~	~~Inhalt der Challenge an das Authenticator-Modul~~	~~gemSpec_IDP_Dienst~~
~~A_20523~~	~~Zusammenstellung der Claims zum "user_consent"~~	~~gemSpec_IDP_Dienst~~
~~A_20524~~	~~Befüllen der Claims "given_name", "family_name", "organizationName", "professionOID" und "idNummer"~~	~~gemSpec_IDP_Dienst~~
~~A_20583~~	~~IdP-Dienst – Sicherung zum Transportnetz Internet durch Paketfilter~~	~~gemSpec_IDP_Dienst~~
~~A_20584~~	~~IdP-Dienst – Platzierung des Paketfilters Internet~~	~~gemSpec_IDP_Dienst~~
~~A_20585~~	~~IdP-Dienst – Richtlinien für den Paketfilter zum Internet~~	~~gemSpec_IDP_Dienst~~
~~A_20586-01~~	~~IdP-Dienst – Verhalten bei Vollauslastung~~	~~gemSpec_IDP_Dienst~~
~~A_20587~~	~~IdP-Dienst – Richtlinien zum TLS-Verbindungsaufbau~~	~~gemSpec_IDP_Dienst~~
~~A_20589~~	~~IdP-Dienst – Ausschluss bestimmter Clientsystem-Versionsnummern von der Kommunikation~~	~~gemSpec_IDP_Dienst~~
~~A_20590~~	~~IdP-Dienst – Ausschluss von Clientsystem-Versionen~~	~~gemSpec_IDP_Dienst~~
~~A_20686~~	~~Erweiterte Nutzung von Schlüsseln~~	~~gemSpec_IDP_Dienst~~
~~A_20687~~	~~Bereitstellung der PUK~~	~~gemSpec_IDP_Dienst~~
~~A_20691~~	~~Das Discovery-Document ist maximal 24 Stunden alt~~	~~gemSpec_IDP_Dienst~~
~~A_20692~~	~~Maximale Gültigkeitsdauer einer "SUBJECT_SESSION"~~	~~gemSpec_IDP_Dienst~~
~~A_20693~~	~~Senden des "AUTHORIZATION_CODE" und "SSO_TOKEN" an die "REDIRECT_URI"~~	~~gemSpec_IDP_Dienst~~
~~A_20694~~	~~Zusammenstellung des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20695~~	~~Signieren des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20698~~	~~Annahme des Authorization-Request~~	~~gemSpec_IDP_Dienst~~
~~A_20699~~	~~Annahme der signierten "CHALLENGE"~~	~~gemSpec_IDP_Dienst~~
~~A_20732~~	~~Aufnahme der öffentlichen Schlüssel in das Discovery Document~~	~~gemSpec_IDP_Dienst~~
~~A_20742~~	~~Vergabe der "client_id" durch den IdP-Dienst~~	~~gemSpec_IDP_Dienst~~
~~A_20946~~	~~Annahme eines "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20948~~	~~Validierung des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20950~~	~~Positive Validierung des "SSO_TOKEN"~~	~~gemSpec_IDP_Dienst~~
~~A_20951~~	~~Validierung der Signatur und des Zertifikats der "CHALLENGE"~~	~~gemSpec_IDP_Dienst~~
~~A_20952~~	~~Claim "aud" im Token setzen~~	~~gemSpec_IDP_Dienst~~
~~A_19908-01~~	~~Authenticator-Modul: Prüfung der Signatur des "CHALLENGE_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20068-01~~	~~Authenticator-Modul: Prüfung Internet-Zertifikate~~	~~gemSpec_IDP_Frontend~~
~~A_20499~~	~~Authenticator-Modul: Temporäre Speicherung von "SSO_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20525~~	~~Authenticator-Modul: Anzeige des "user_consent" und PIN-Abfrage~~	~~gemSpec_IDP_Frontend~~

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20526~~	~~Authenticator-Modul: Response auf die "CHALLENGE" des Authorization-Endpunktes~~	~~gemSpec_IDP_Frontend~~
~~A_20527~~	~~Authenticator-Modul: Übertragung des "AUTHORIZATION_CODE" an das Anwendungsfrontend~~	~~gemSpec_IDP_Frontend~~
~~A_20600~~	~~Authenticator-Modul: Annahme des "user_consent" und des "CHALLENGE_TOKEN"~~	~~gemSpec_IDP_Frontend~~
~~A_20601~~	~~Authenticator-Modul: Übergabe des Authorization-Request an den Authorization-Endpunkt~~	~~gemSpec_IDP_Frontend~~
~~A_20607~~	~~Authenticator-Modul: Kommunikation über TLS-Verbindung~~	~~gemSpec_IDP_Frontend~~
~~A_20609~~	~~Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen~~	~~gemSpec_IDP_Frontend~~
~~A_20614~~	~~Authenticator-Modul: Prüfung der Signatur des Discovery Document~~	~~gemSpec_IDP_Frontend~~
~~A_20617-01~~	~~Authenticator-Modul: Verpflichtende Zertifikatsprüfung~~	~~gemSpec_IDP_Frontend~~
~~A_20618~~	~~Authenticator-Modul: Unzulässige TLS-Verbindungen ablehnen~~	~~gemSpec_IDP_Frontend~~
~~A_20700-04~~	~~Authenticator-Modul: Signatur der "CHALLENGE"~~	~~gemSpec_IDP_Frontend~~
~~A_20574~~	~~Beachtung der ISI LANA für Übergänge zu Fremdnetzen~~	~~gemSpec_Net~~
~~GS-A_4062-01~~	~~Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen~~	~~gemSpec_Net~~

4 Anhang – Verzeichnisse

4.1 Abkürzungen

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

4.2 Tabellenverzeichnis

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