

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Sektoraler Identity Provider

Produkttyp Version: 2.0.3-0
Produkttyp Status: freigegeben

Version: 1.0.0
Revision: 706401
Stand: 01.09.23
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_IDP-Sek_PTV_2.0.3-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

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

| Produkttypversion | Beschreibung der Änderung | Referenz |
|-------------------|---|---------------------------------|
| 1.0.0-0 | initiale Version | gemProdT_IDP- Sek_PTV1.0.0-0 |
| 1.0.1-0 | Anpassung aufgrund der Einarbeitung der Änderungen aus Betr_Maintenance_21.3 sowie Anpassungen an [gemSpec_SST_LD_BD] | gemProdT_IDP- Sek_PTV1.0.1-0 |
| 1.0.2-0 | Anpassung aufgrund der Einarbeitung der Änderungen aus Betr_Maintenance_22.1 | gemProdT_IDP- Sek_PTV1.0.2-0 |
| 2.0.0-0 | Anpassung aufgrund der Einarbeitung Feature IDP-Federation | gemProdT_IDP- Sek_PTV2.0.0-0 |
| 2.0.0-1 | Anpassung aufgrund der gemSpec_Perf Version Änderung | gemProdT_IDP- Sek_PTV2.0.0-1 |
| 2.0.1-0 | Anpassung aufgrund der Einarbeitung der Änderungen aus IDP_Maintenance_23.1 | gemProdT_IDP- Sek_PTV2.0.1-0 |
| 2.0.2-0 | Anpassung aufgrund der Einarbeitung der Änderungen aus IDP_23.3 | gemProdT_IDP- Sek_PTV2.0.2-0 |
| 2.0.3-0 | Anpassung aufgrund der Einarbeitung der Änderungen aus IDP_23.4 | gemProdT_IDP- Sek_PTV2.0.3-0 |

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 | 01.09.23 | | freigegeben | gematik |

Inhaltsverzeichnis

| | |
|--|-----------|
| 1 Einführung | 5 |
| 1.1 Zielsetzung und Einordnung des Dokumentes | 5 |
| 1.2 Zielgruppe | 5 |
| 1.3 Geltungsbereich | 5 |
| 1.4 Abgrenzung des Dokumentes | 5 |
| 1.5 Methodik | 6 |
| 2 Dokumente | 7 |
| 3 Normative Festlegungen | 9 |
| 3.1 Festlegungen zur funktionalen Eignung..... | 9 |
| 3.1.1 Produkttest/Produktübergreifender Test | 9 |
| 3.1.2 Herstellererklärung funktionale Eignung | 11 |
| 3.2 Festlegungen zur sicherheitstechnischen Eignung | 15 |
| 3.2.1 Herstellererklärung sicherheitstechnische Eignung..... | 15 |
| 3.2.2 Sicherheitsgutachten | 16 |
| 3.2.3 Produktgutachten | 17 |
| 4 Produktypspezifische Merkmale | 20 |
| 5 Anhang – Verzeichnisse | 21 |
| 5.1 Abkürzungen | 21 |
| 5.2 Tabellenverzeichnis | 21 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

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

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

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an Hersteller und Anbieter von sektoralen Identity Providern 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) und
- Auditoren.

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

1.3 Geltungsbereich

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

1.4 Abgrenzung des Dokumentes

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

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) entnommen werden.

1.5 Methodik

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

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

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

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|-----------------------|--|---------|
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.28.0 |
| gemSpec_DS_Hersteller | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller | 1.5.0 |
| gemSpec_OM | Übergreifende Spezifikation Operations und Maintenance | 1.15.0 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.15.0 |
| gemSpec_Perf | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform | 2.301.0 |
| gemKPT_Test | Testkonzept der TI | 2.8.7 |
| gemSpec_IDP_Sek | Spezifikation Sektoraler Identity Provider | 2.2.0 |

Die Bestätigungs-/Zulassungsbedingungen für das Bestätigungs-/Zulassungsobjekt "Sektoraler Identity Provider" werden im Dokument [gemZul_Prod_IDP_Sek] im Downloadcenter der gematik im Abschnitt "Zulassungen und Bestätigungen durch die gematik" veröffentlicht.

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

Tabelle 2: Informative Dokumente und Web-Inhalte

| Quelle | Herausgeber: Bezeichnung / URL | Version Branch / Tag |
|---|---|----------------------------|
| [gemRL_Pruef SichEig_DS] | gematik: Richtlinie zur Prüfung der Sicherheitseignung | 2.2.0 |
| [The OAuth 2.0 Authorization Framework] | IETF: https://www.rfc-editor.org/rfc/rfc6749.html | |

| Quelle | Herausgeber: Bezeichnung / URL | Version Branch / Tag |
|---|--|----------------------------|
| [Proof Key for Code Exchange by OAuth Public Clients] | IETF: https://datatracker.ietf.org/doc/html/rfc7636 | |
| [OAuth 2.0 Pushed Authorization Requests] | IETF: https://www.rfc-editor.org/rfc/rfc9126.html | |
| [OpenID Connect Core 1.0] | OpenID Connect Working Group: https://openid.net/specs/openid-connect-core-1_0.html | |
| [OpenID Connect Federation 1.0] | OpenID Connect Working Group: https://openid.net/specs/openid-connect-federation-1_0.html | |
| [TR-03107-1] | BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf | |

Hinweis:

- Ist kein Herausgeber angegeben, wird angenommen, dass die gematik für Herausgabe und Veröffentlichung der Quelle verantwortlich ist.
- Ist keine Version angegeben, bezieht sich die Quellenangabe auf die aktuellste Version.
- Bei Quellen aus gitHub werden als Version Branch und / oder Tag verwendet.

3 Normative Festlegungen

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

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

| ID | Bezeichnung | Quelle (Referenz) |
|------------|---|-------------------|
| A_22257 | Operationsaufruf erfordert erfolgreiche Authentifizierung | gemSpec_IDP_Sek |
| A_22321 | Prüfung des "CODE_VERIFIER" | gemSpec_IDP_Sek |
| A_22324 | Verwendung des Attributes "state" durch sektoralen IDP | gemSpec_IDP_Sek |
| A_22325-01 | Übermitteln des "AUTHORIZATION_CODE" an den Sender des Requests | gemSpec_IDP_Sek |
| A_22643 | Entity Statement des sektoralen IDP | gemSpec_IDP_Sek |
| A_22651 | Parameter des Pushed Authorization Request durch den sektoralen IDP | gemSpec_IDP_Sek |
| A_22653 | Annahme von "AUTHORIZATION_CODE" und "CODE_VERIFIER" | gemSpec_IDP_Sek |
| A_22654 | Prüfung des TLS Clientzertifikates am Token-Endpunkt des sektoralen IDP | gemSpec_IDP_Sek |
| A_22655-01 | Signatur des "ID_TOKEN" des sektoralen IDP | gemSpec_IDP_Sek |
| A_22706 | "ID_TOKEN" des sektoralen IDP | gemSpec_IDP_Sek |
| A_22711 | Regelmäßige Erneuerung des Entity Statement des sektoralen IDP | gemSpec_IDP_Sek |
| A_22744 | Authenticator auf Zweitgerät | gemSpec_IDP_Sek |

| ID | Bezeichnung | Quelle (Referenz) |
|------------|---|--------------------------|
| A_22922 | Anfragen veralteter Authenticator Versionen | gemSpec_IDP_Sek |
| A_22931 | Zu verwendende Produktversion in der Kommunikation zum IDP | gemSpec_IDP_Sek |
| A_22939 | Widerspruch zur Weitergabe einzelner Scopes | gemSpec_IDP_Sek |
| A_22966 | Prüfung eingehender Pushed Authorization Request durch den sektoralen IDP | gemSpec_IDP_Sek |
| A_22983 | Signaturverfahren für Signatur des "ID_TOKEN" des sektoralen IDP | gemSpec_IDP_Sek |
| A_22989 | "scopes" und "claims" des sektoralen IDP für Versicherte | gemSpec_IDP_Sek |
| A_22990 | Umgang mit fehlenden oder verwehrt Informationen | gemSpec_IDP_Sek |
| A_22991 | Prüfung des TLS Clientzertifikates am PAR-Endpunkt des sektoralen IDP | gemSpec_IDP_Sek |
| A_22992 | Antwort auf einen eingehenden Pushed Authorization Request durch den sektoralen IDP | gemSpec_IDP_Sek |
| A_22993 | Gültigkeit der vom sektoralen IDP erstellten Request-URI | gemSpec_IDP_Sek |
| A_23007 | Gültigkeit des "AUTHORIZATION_CODE" | gemSpec_IDP_Sek |
| A_23010 | Maximale Gültigkeitsdauer eines Entity Statement des sektoralen IDP | gemSpec_IDP_Sek |
| A_23031 | Authenticator-Modul: OAuth 2.0 Pushed Authorization Request (PAR) | gemSpec_IDP_Sek |
| A_23132 | Regelmäßige Aktualisierung der Entity Statements bekannter Fachdienste | gemSpec_IDP_Sek |
| A_23133 | Maximale Gültigkeitsdauer der Entity Statements bekannter Fachdienste | gemSpec_IDP_Sek |
| A_23162 | Invalidisierung des "AUTHORIZATION_CODE" | gemSpec_IDP_Sek |
| A_23413 | Entity Statement vom Federation Master abrufen | gemSpec_IDP_Sek |
| A_21275-01 | TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake | gemSpec_Krypt |
| A_21332 | E-Rezept: TLS-Vorgaben | gemSpec_Krypt |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------------------|---|-------------------------|
| GS-A_4543 | Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten | gemSpec_OM |
| GS-A_4662 | Bedingungen für TLS-Handshake | gemSpec_PKI |
| A_21980 | Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22000 | Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22002 | Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22004 | Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22429 | Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22825-01 | Performance - Rohdaten - Spezifika sektoraler IDP - Operation/Duration (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22944 | Performance - Rohdaten - Spezifika föderierter IDP - Message (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22012-02 | Performance - Rohdaten - Spezifika IDP - Duration (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22825 | Performance - Rohdaten - Spezifika - Operation (Rohdatenerfassung v.02) | gemSpec_Perf |

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|--|-------------------|
| A_20065 | Nutzung der Dokumententemplates der gematik | gemKPT_Test |
| GS-A_2162 | Kryptographisches Material in Entwicklungs- und Testumgebungen | gemKPT_Test |

| ID | Bezeichnung | Quelle (Referenz) |
|----------------|--|--------------------------|
| TIP1-A_2775 | Performance in RU | gemKPT_Test |
| TIP1-A_2805 | Zeitnahe Anpassung von Produktkonfigurationen | gemKPT_Test |
| TIP1-A_4191 | Keine Echtdaten in RU und TU | gemKPT_Test |
| TIP1-A_5052 | Dauerhafte Verfügbarkeit in der RU | gemKPT_Test |
| TIP1-A_6079 | Updates von Referenzobjekten | gemKPT_Test |
| TIP1-A_6080 | Softwarestand von Referenzobjekten | gemKPT_Test |
| TIP1-A_6081 | Bereitstellung der Referenzobjekte | gemKPT_Test |
| TIP1-A_6082 | Versionen der Referenzobjekte | gemKPT_Test |
| TIP1-A_6085 | Referenzobjekte eines Produkts | gemKPT_Test |
| TIP1-A_6088 | Unterstützung bei Fehlernachstellung | gemKPT_Test |
| TIP1-A_6517-01 | Eigenverantwortlicher Test: TBI | gemKPT_Test |
| TIP1-A_6518 | Eigenverantwortlicher Test: TDI | gemKPT_Test |
| TIP1-A_6519 | Eigenverantwortlicher Test: Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6523 | Zulassungstest: Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6524-01 | Testdokumentation gemäß Vorlagen | gemKPT_Test |
| TIP1-A_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_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 |

| ID | Bezeichnung | Quelle (Referenz) |
|-------------|--|--------------------------|
| TIP1-A_7334 | Risikoabschätzung bezüglich der Interoperabilität | gemKPT_Test |
| TIP1-A_7335 | Bereitstellung der Testdokumentation | gemKPT_Test |
| A_22253 | Ausschluss bestimmter Authenticator-Modul Versionen von der Kommunikation | gemSpec_IDP_Sek |
| A_22254-01 | Ausschluss von Authenticator-Modul Versionen (Rohdatenerfassung v.02) | gemSpec_IDP_Sek |
| A_22308-01 | Beschränkung des Authenticator-Moduls eines sektoralen IDP auf die Authentifizierung | gemSpec_IDP_Sek |
| A_22311 | Verwendung der ursprünglichen Adresse zur Übergabe des "AUTHORIZATION_CODE" | gemSpec_IDP_Sek |
| A_22312-01 | Einhaltung der Standards bei der Realisierung des Authorization-Endpunkts | gemSpec_IDP_Sek |
| A_22316 | Maximale Gültigkeitsdauer von "ID_TOKEN" | gemSpec_IDP_Sek |
| A_22323 | Protokollierung der Token-Ausgabe in allen Fällen | gemSpec_IDP_Sek |
| A_22659 | Realisierung der App2App-Kommunikation im Fall Android | gemSpec_IDP_Sek |
| A_22660 | Realisierung der App2App-Kommunikation im Fall Apple/iOS | gemSpec_IDP_Sek |
| A_22712 | Unterstützung von NFC eGK und PIN | gemSpec_IDP_Sek |
| A_22713 | Unterstützung des elektronischen Identitätsnachweis (online-Ausweisfunktion) | gemSpec_IDP_Sek |
| A_23055 | Aufbau RU-Instanz | gemSpec_IDP_Sek |
| A_23056 | Bereitstellung der TU-Instanz | gemSpec_IDP_Sek |
| A_23163 | Anpassung RU-Instanz | gemSpec_IDP_Sek |
| A_23623 | Wahlfreiheit des Authentisierungsverfahren für TI-Anwendungen | gemSpec_IDP_Sek |
| A_18464 | TLS-Verbindungen, nicht Version 1.1 | gemSpec_Krypt |
| A_18467 | TLS-Verbindungen, Version 1.3 | gemSpec_Krypt |
| GS-A_4385 | TLS-Verbindungen, Version 1.2 | gemSpec_Krypt |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern | gemSpec_OM |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|--------------------------|
| GS-A_3696 | Zeitpunkt der Erzeugung neuer Versionsnummern | gemSpec_OM |
| GS-A_3697 | Anlass der Erhöhung von Versionsnummern | gemSpec_OM |
| GS-A_3813 | Datenschutzvorgaben Fehlermeldungen | gemSpec_OM |
| GS-A_4541 | Nutzung der Produkttypversion zur Kompatibilitätsprüfung | gemSpec_OM |
| GS-A_4542 | Spezifikationsgrundlage für Produkte | gemSpec_OM |
| GS-A_5038 | Festlegungen zur Vergabe einer Produktversion | gemSpec_OM |
| GS-A_5039-01 | Änderung der Produktversion bei Änderungen der Produkttypversion | gemSpec_OM |
| GS-A_5040-01 | Änderung der Produktversion bei Produktänderungen außerhalb von Produkttypänderungen | gemSpec_OM |
| GS-A_5054 | Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen | gemSpec_OM |
| A_21975 | Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_21976 | Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_21978 | Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_21979 | Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_21981-02 | Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_21982-01 | Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22001-01 | Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22005 | Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22047 | Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02) | gemSpec_Perf |

| ID | Bezeichnung | Quelle (Referenz) |
|------------|---|-------------------|
| A_22482 | Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22500-01 | Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22504 | Performance - Rohdaten - Spezifika IDP - Feldtrennzeichen im Useragent (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22513-01 | Performance - Rohdaten - Message-Block im Fehlerfall (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22826 | Performance - Rohdaten - Spezifika sektoraler IDP - Status (Rohdatenerfassung v.02) | gemSpec_Perf |

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Herstellererklärung sicherheitstechnische Eignung

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

Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|-----------------------|
| A_17179 | Auslieferung aktueller zusätzlicher Softwarekomponenten | gemSpec_DS_Hersteller |
| A_19164 | Mitwirkungspflicht bei Sicherheitsprüfung | gemSpec_DS_Hersteller |
| A_19165 | Auditrechte der gematik zur Prüfung der Herstellerbestätigung | gemSpec_DS_Hersteller |
| A_23445 | Beteiligung der Hersteller am Coordinated Vulnerability Disclosure Programm | gemSpec_DS_Hersteller |
| GS-A_2330-02 | Hersteller: Schwachstellen-Management | gemSpec_DS_Hersteller |
| GS-A_2525-01 | Hersteller: Schließen von Schwachstellen | gemSpec_DS_Hersteller |
| GS-A_4944-01 | Produktentwicklung: Behebung von Sicherheitsmängeln | gemSpec_DS_Hersteller |
| GS-A_4945-01 | Produktentwicklung: Qualitätssicherung | gemSpec_DS_Hersteller |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|--|-----------------------|
| GS-A_4946-01 | Produktentwicklung: sichere Programmierung | gemSpec_DS_Hersteller |
| GS-A_4947-01 | Produktentwicklung: Schutz der Vertraulichkeit und Integrität | gemSpec_DS_Hersteller |
| A_22649 | Anfragen unbekannter Clients | gemSpec_IDP_Sek |
| A_22690 | Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Betriebshandbuch | gemSpec_IDP_Sek |
| 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_18986 | Fachdienst-interne TLS-Verbindungen | gemSpec_Krypt |
| GS-A_5542 | TLS-Verbindungen (fatal Alert bei Abbrüchen) | gemSpec_Krypt |
| GS-A_5580-01 | TLS-Klient für betriebsunterstützende Dienste | gemSpec_Krypt |

3.2.2 Sicherheitsgutachten

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

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

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

| ID | Bezeichnung | Quelle (Referenz) |
|---------|--|-----------------------|
| 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_22984 | Unverzügliche Bewertung von Schwachstellen | gemSpec_DS_Hersteller |
| A_22985 | Bereitstellung der Bewertung von Schwachstellen gegenüber der gematik | gemSpec_DS_Hersteller |
| A_22986 | Meldung von erheblichen Schwachstellen und Bedrohungen | gemSpec_DS_Hersteller |
| A_23029 | Bereitstellung von Updates abhängig von der Kritikalität der Schwachstellen | gemSpec_DS_Hersteller |
| A_21332 | E-Rezept: TLS-Vorgaben | gemSpec_Krypt |

3.2.3 Produktgutachten

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

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"

| ID | Bezeichnung | Quelle (Referenz) |
|---------|---|-------------------|
| A_22650 | automatische Registration von Fachdiensten | gemSpec_IDP_Sek |
| A_22830 | sektoraler IDP – Verarbeitungskontext der VAU | gemSpec_IDP_Sek |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|--------------------------|
| A_22832 | Authenticator-Modul: Anzeige des "user_consent" | gemSpec_IDP_Sek |
| A_22840 | Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten | gemSpec_IDP_Sek |
| A_22841 | Schutz der Persistenzschlüssel durch ein HSM | gemSpec_IDP_Sek |
| A_22842 | Bereitstellung Persistenzschlüssel | gemSpec_IDP_Sek |
| A_22843 | Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU | gemSpec_IDP_Sek |
| A_22844 | Transportverschlüsselte Übertragung von Daten mit Fachdiensten | gemSpec_IDP_Sek |
| A_22847 | Authentisierung gegenüber Clients | gemSpec_IDP_Sek |
| A_22848 | Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU | gemSpec_IDP_Sek |
| A_22849 | Isolation der VAU von Datenverarbeitungsprozessen des Anbieters | gemSpec_IDP_Sek |
| A_22850 | Ausschluss von Manipulationen an der Software der VAU | gemSpec_IDP_Sek |
| A_22851 | Ausschluss von Manipulationen an der Hardware der VAU | gemSpec_IDP_Sek |
| A_22852 | Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU | gemSpec_IDP_Sek |
| A_22853 | Ausschluss von Manipulationen über physische Angriffe | gemSpec_IDP_Sek |
| A_22854 | Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU | gemSpec_IDP_Sek |
| A_22855 | HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU | gemSpec_IDP_Sek |
| A_22856 | Konsistenter Systemzustand des Verarbeitungskontextes der VAU | gemSpec_IDP_Sek |
| A_22864 | Umsetzung von Operationen in einer Vertrauenswürdigem Ausführungsumgebung (VAU) | gemSpec_IDP_Sek |
| A_22868 | Private Schlüssel im HSM | gemSpec_IDP_Sek |

| ID | Bezeichnung | Quelle (Referenz) |
|------------|--|--------------------------|
| A_22978 | Aufbereiten von Geräteinformationen | gemSpec_IDP_Sek |
| A_23018 | Anforderungen an den Schutz vor Profilbildung | gemSpec_IDP_Sek |
| A_23193-01 | Verschlüsseln der "ID_TOKEN" | gemSpec_IDP_Sek |
| A_23197 | Nutzung eines pairwise Subject als Pseudonym des Versicherten | gemSpec_IDP_Sek |
| A_23337 | Mindestvorgaben für Schlüssel von sektoralen IDPs als Teilnehmer der TI-Föderation | gemSpec_IDP_Sek |
| A_23389 | Authenticator-Modul: Schutz vor Missbrauch | gemSpec_IDP_Sek |

4 Produktypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produktyps vor.

5 Anhang – Verzeichnisse

5.1 Abkürzungen

| Kürzel | Erläuterung |
|--------|-----------------|
| ID | Identifikation |
| CC | Common Criteria |
| ST | Security Target |

5.2 Tabellenverzeichnis

| | |
|---|----|
| Tabelle 1: Dokumente mit normativen Festlegungen | 7 |
| Tabelle 2: Informative Dokumente und Web-Inhalte | 7 |
| Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" | 9 |
| Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellereklärung" | 11 |
| Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Herstellereklärung" | 15 |
| Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" | 16 |
| Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten" | 17 |