Fragen & Antworten (FAQ)

	Fragen & Antworten zu den fachlichen & technischen Themen der TI-Föderation
1	Gibt es eine Spezifikation bzw. Dokumente, an denen man sich orientieren kann? Die Spezifikationen zur TI-Föderation werden im Fachportal der gematik veröffentlicht. Die Spezifikation der sektoralen IDPs ist vorerst begrenzt auf die Authentifizierung von Versicherten. Die Anforderungen an sektorale IDPs für Leistungserbringer und Leistungserbringerinstitutionen sind derzeit in Vorbereitung. Zusätzliche Dokumentationen zum Identity Management finden Sie in der IDP Wissensdatenbank.
2	Warum existiert given_name, nicht aber last name? Was war hier die Intention? Der claim *given_name* wurde aufgrund von DiGA-Anforderung mit aufgenommen. Nach den Vorgaben BfArM - DiGA und DiPA Datenschutzkriterien dürfen DiGAs höchstens den Vornamen verwenden. Deshalb wurde der claim *given_name* als gesondertes Objekt aufgenommen, um zumindest für diesen die Bereitstellung über den sektoralen IDP zu ermöglichen.
3	Wie genau soll die Identifikation und Authentisierung mittels nPA erfolgen? Für die erstmalige eindeutige Identifikation kann ein Diensteanbieter durch die Online-Ausweisfunktion (eID-Funktion) die folgend aufgeführten Attribute des Ausweisinhabers ausgelesen werden: • Familienname • Vornamen • Geburtsname • Doktorgrad • Tag der Geburt • Ort der Geburt • Anschrift Diese Daten können verwendet werden, um den Anwender eindeutig einem Datensatz im Bestand des IDP/des Kostenträgers zuzuordnen. Für die folgenden Authentisierungen reicht es aus, das *dienste- und kartenspezifische Kennzeichen* (wie z.B. die Personalausweisnummer) zu verwenden, mit welchem der Anwender eindeutig wiedererkannt werden kann. Zu beachten ist, dass sich das *dienste- und kartenspezifische Kennzeichen* nach Neuausstellung ändert, die Zuordnung also erneut erfolgen muss.

4	Wie soll eine eGK bei Identifikation/Authentisierung geprüft werden? Konkrete Anforderungen und eine Dokumentation für einen einzelnen Verpflichtenden Weg gibt es keine. Die gematik hat sich bewusst entschieden den Herstellern hier Freiheiten zu lassen. Orientieren kann man sich natürlich an dem Prozess wie er beim IDP-Dienst für diese Funktionalität umgesetzt ist. Dabei wird eine an das Authenticator Modul gesendete Challenge mittels eGK Signiert und diese Antwort (Signatur und verschlüsseltes Zertifikat) dann geprüft auf zeitliche und kryptographische Gültigkeit sowie das verwendete Zertifikat mittels OCSP Anfrage beim TSP validiert. Die relevanten Anforderung dazu sind in gemSpec_IDP-Dienst (A_20521-02, A_20314-01, A_20699-03, A_20951-01, A_22328, A_22290, A_20465) und in gemSpec_IDP_Frontend (A_20525, A_19908-01, A_20700-07, A_20526-01) formuliert. Die Spezifikationsdokumente können aus dem Fachportal runtergeladen werden. Hier wären aber explizit auch andere Wege der Gültigkeitsprüfung gegen die Systeme der Krankenkasse möglich und sinnvoll. So wäre es nicht notwendig das Zertifikat der eGK verschlüsselt zum sektoralen IDP zu übertragen, wenn dieser die Informationen zum Nutzer in einem eigenen Datenbestand vorhalten und im Backend mit der Kasse abgleichen. Es kann also durchaus ausreichen die Challenge zu signieren und den öffentlichen Schlüssel zu übertragen mit welchem der IDP alle weiteren Daten in seiner Datenbank findet.
5	Der gematik-App-2-App-Flow betrachtet keine Rücksprünge zur TI-App bei Fehlern in Authentifizierung oder Abbruch. Wird diese Lücke noch geschlossen? Im Rahmen der mittels der App2App-Link-kommunizierten Parameter können auch OAuth konforme Error-Codes und Error-Descriptions als Parameter vom Authenticator-Modul an das Frontend übermittelt werden. Im nächsten überarbeiteten Release der Spezifikation sollen Aspekte zur Fehlerbehandlung ergänzt werden, damit für das Anwendungsfrontend bzw. den aufrufenden Fachdienst deutlich wird, welche Fehlercodes zu erwarten sind und für den sektoralen IDP klargestellt wird, dass diese vom Authenticator-Modul weitergereicht werden müssen. So kann eine Anwendung entsprechend reagieren und ggf. eine erneute Authentisierung anstoßen oder den Nutzer über Probleme informieren.
6	Ist es möglich, die Gerätebindung durch Schlüsseltausch ohne Nutzerinteraktion durchzuführen? Die aktuelle Spezifikation lässt Interpretationsspielraum zur Erneuerung der Gerätebindung. Der Aspekt ist aber weiterhin auch mit dem BSI in Diskussion. Daher ist eine Umsetzung einer neuen Gerätebindung durch Verwendung der alten Gerätebindung mit einem gewissen Risiko behaftet. Die Erneuerung der Gerätebindung ohne Nutzerbestätigung ist in keinem Fall erlaubt.
7	eID und eGK werden als alternative Authentverfahren in der Spezifikation aufgeführt. Inwiefern müssen/sollen diese Verfahren unabhängig vom Anlegen eines Benutzeraccounts funktionieren? Die anzubietenden Identifikationsverfahren und Authentisierungsverfahren "eGK mit PIN" und "Online Ausweisfunktion" müssen unabhängig vom Anlegen eines Benutzeraccounts möglich sein. Benutzeraccounts können/müssen eingerichtet werden, um ein eindeutiges Mapping der "Online Ausweisfunktion" auf einen Versicherten zu vollziehen. Diese haben allerdings nicht zwingend ein gesondertes Authentisierungsverfahren, sondern müssen auf Wunsch des Nutzers die Anmeldung an den TI-Fachdiensten lediglich über das gewählte Authentisierungsmittel (eID/eGK) beschränken. Werden neben den geforderten Verfahren "elektronischer Identitätsnachweis" (A_22713) bzw. "eGK+PIN" (A_22712) verpflichtend weitere Authentifizierungsverfahren für einen Nutzer eingerichtet, so muss dem Nutzer die Möglichkeit gegeben werden auszuwählen, welche Verfahren für die Authentisierung bei TI-Fachanwendungen verwendet werden dürfen. Dies wird mit der Anforderung A_23623 klargestellt.
8	Welche "Certificate Transparency Log" muss geprüft werden? Die Zertifikate müssen von einer CA bezogen werden, welche die Ausstellung der Zertifikate in einem Certificate Transparency Log protokolliert. Diese Log-Einträge müssen geprüft werden. Für die Prüfung von Logeinträgen zu Domain gibt es eine Reihe von CT-Anbietern. Die gematik schreibt kein bestimmtes CT vor. Wenn die CA ein solches präferiert, so kann das gerne verwendet werden.
9	Die "Tabelle 16 : Body Entity Statement des sektoralen IDP" im gemSpec_IDP_Sek beschreibt den Claim "metadata/openid_provider /signed_jwks_uri" im Body des Entity Statements des sektoralen IDP-s, dieser dient dazu integritätsgeschützt die Signaturschlüssel für die ausgestellten Token des IDP zu verwalten ohne sie direkt in das Entity Statement einzubinden. Ist es möglich, dass ein sektoraler IDP für die Signatur des signed_jwks einen anderen Schlüssel verwendet, als für die Signatur des eigenen Entity Statements? Wenn dies der Fall ist, sind die Betreiber der sektoralen IDPs verpflichtet, diesen Schlüssel am Federation Master zu hinterlegen? Es ist nach Spezifikationslage zulässig, dass der IDP einen anderen Schlüssel zur Signatur des JWT, welches unter signed_jwks_uri abgerufen wird, verwendet, als zur Signatur des Entity Statements. Der Schlüssel muss dann über das Entity Statement im Claim jwks auf Root Ebene transportiert werden (also nicht als Metadatum unter openid_provider). Dieser Schlüssel muss nicht über einen organisatorischen Prozess am FedMaster registriert werden. Seine Verwaltung obliegt allein dem sektoralen IDP.

10	Wie ist der Zusammenhang zwischen Gültigkeit der Identifizierung und Gültigkeit der zur Identifizierung eingesetzten Ausweisdokumenten? • Ein Identifizierungsvorgang mit einem entsprechenden Ausweisdokument (nPA, eGK) ist möglich bis einschließlich zum letzten Tag der Gültigkeit des Ausweis-Dokuments. • Der Zeitraum der Gültigkeit der Identifizierung (abhängig von der Geräteklasse, z.B. sechs Monate) ist nicht abhängig von der noch verbleibenden Gültigkeit des Ausweisdokuments zum Zeitpunkt der Identifizierung. • Ein Anmeldevorgang (Authentisierung) mit einem entsprechenden Ausweisdokument (nPA, eGK) ist möglich bis einschließlich zum letzten Tag der Gültigkeit des Ausweis-Dokuments.
11	Die Liste der zulässigen Identifikationsverfahren (https://fachportal.gematik.de/schnelleinstieg/smartcards-und-identitaeten-in-der-ti/identitaeten) ist auch das Identifikationsverfahren "Persönliche Identifikation in der Geschäftsstelle der Krankenkasse" enthalten. Das Identifikationsverfahren erfüllt formell nicht die Anforderung an das Schutzniveau "hoch". Kann des Verfahren als Identifikationsverfahren die Gesundheits-ID? Aktuell werden über das Identifikationsverfahren "Persönliche Identifikation in der Geschäftsstelle der Krankenkasse" Fälle abgedeckt, für die es derzeit keine Alternativen gibt (Kinder, bevollmächtigte Vertreter). Wir als gematik gehen davon aus, dass das Verfahren "Persönliche Identifikation in der Geschäftsstelle der Krankenkasse" bis zu einer möglichen Konkretisierung der Rahmenbedingungen ein zulässiges Identifikationsverfahren sowohl für die PIN-Herausgabe wie auch die Gesundheits-ID bleibt.
	Fragen & Antworten zu normativen Anforderungen aus den Spezifikationen
12	Die Anforderung A_22649 beschreibt, dass, sofern der Client nicht bekannt ist, 401 als Error Response zurückgegeben und intern die automatische Client-Registrierung angestoßen wird. Wie wird der Client aber darüber informiert, wenn diese Registrierung nicht möglich ist, weil z.B. die TrustChain nicht validiert werden kann? Es ist für einen IDP auch zulässig, nach einer fehlgeschlagenen Registrierung weiterhin den HTTP-Fehlercode 401 zu liefern, da die TLS-Aushandlung ohne vertrauenswürdige Schlüssel fehlschlägt. Fehler gemäß OIDC Federation Standard kommen erst innerhalb der TLS-Verbindung zum Tragen. Dies ist für den aufrufenden Fachdienst nicht optimal, aber dieser kann über das ITSM der TI eine Problemlösung veranlassen.
13	Wie kommt der Fachdienst zu seinem Zertifikat für die mTLS-Kommunikation mit dem IDP (A_23183)? Der Fachdienst kann selbst signierte (self-signed) Zertifikate erstellen oder TLS-Client-Zertifikate aus einer CA beziehen. Aus einer CA bezogene Zertifikate werden durch den sektoralen IDP nicht gegen einen TSP geprüft. Es wird lediglich das konkrete Zertifikat gegen die validen Zertifikate aus dem Entity-Statement des Fachdienstes abgeglichen.
14	Erstreckt sich der Anwendungsbereich von GS-A_4367 (Zufallszahlengenerator) und GS-A_4368 (Schlüsselerzeugung) auch auf die Erzeugung von Schlüsseln des Nutzers, welche im Rahmen des Authentifizierungsmechanismus im mobilen Endgerät des Nutzers erzeugt/gespeichert werden? Nein. Eine Nachweis für die Erzeugung von Schlüsseln im Rahmen der Gerätebindung (siehe dazu Anforderung A_22750) gemäß GS-A_4367 / GS-A_4368 ist nicht notwendig.
15	Gelten die Vorgaben aus GS-A_4367 auf für die Schlüsselerzeugung auf dem Mobilen Endgerät - etwa zur Gerätebindung und müssen entsprechende Nachweise erbracht werden? Die Vorgaben aus GS-A_4367 gelten nicht für das Mobile Endgerät sondern nur für Schlüssel der Serverkomponenten innerhalb der VAU. Der Sicherheit der Schlüssel auf dem Mobilgerät wird über die Vorgaben zum Schlüsselwechsel Rechnung getragen.

16	Welches Schlüsselmaterial liegt im Anwendungsbereich der Anforderung A_23337? Erstreckt sich der Anwendungsbereich dieser Anforderung auch auf die Schlüsselerzeugung bzw. dafür genutzte Zufallsgeneratoren? Der Anwendungsbereich erstreckt sich ausschließlich auf Schlüsselmaterial, welches im Rahmen der Kommunikation zwischen dem sektoralem IDP und anderen Teilnehmern der Föderation Anwendung findet: • Signaturen von (ID-)Token, Entity Statement • TLS-Verbindungen zu Teilnehmern der TI-Föderation TLS-Clientschlüssel Schlüsselmaterial hinsichtlich der Kommunikation zwischen Komponenten innerhalb des sektoralen IDP liegt nicht im Anwendungsbereich dieser Anforderung. Schlüsselmaterial betreffend des Authentifizierungsmechanismus zur Authentifizierung des Nutzers liegt nicht im Anwendungsbereich dieser Anforderung (siehe dazu die Anforderungen A_23025 und A_23024). Der Anwendungsbereich der Anforderung erstreckt sich nicht auf die Schlüsselerzeugung bzw. dafür genutzte Zufallsgeneratoren. Anforderungen an die Schlüsselerzeugung/Zufallsgeneratoren werden von GS-A_4367 – Zufallszahlengenerator, GS-A_4368 – Schlüsselerzeugung erfasst.
17	Gibt es eine Umsetzungsbeschreibung für die Einbeziehung der gematik (im Sinne von Zeitpunkt, technische Kanäle, Gremien, Dokumentation, Ansprechpartner etc.) bzgl. der Anforderung "A_23205 - Prozesse für die Verwaltung des HSM"? Übernimmt die gematik in dem Prozess einen aktiven Part oder soll lediglich die Möglichkeit der Beobachtung des Prozesses eingeräumt werden? <u>Mehraugenprinzip:</u> Die gematik wird keine aktive Beteiligung im Quorum (Mehraugenprinzip) haben. Ein Quorum kann z. B. durch den Anbieter des sektoralen IDP und eine Krankenkasse als Auftraggeber gebildet werden. Sollte der Anbieter des sektoralen IDP keine unabhängige Stelle finden, mit der ein Quorum gebildet werden kann, bietet die gematik allerdings an, diese Rolle zu übernehmen. <u>Remote-Teilnahme der gematik:</u> Die gematik wird sich bei der Umsetzung vom Mehraugenprinzip (Quorum) in der Regel nicht aktiv beteiligen. Die gematik behält sich jedoch das Recht vor, auf Anfrage über eine Konferenzschaltung die Umsetzung des Prozesses zu beobachten. Für die Sicherstellung der Anforderungserfüllung (Mehraugenprinzip und Remote-Teilnahme) ist eine Prozessdokumentation der Umsetzung ausreichend.
18	Was ist in der Anforderung A_22943 ("Richtlinien zum TLS-Verbindungsaufbau") mit "vereinfachte Zertifikatsprüfung mit TLS-Standardbibliotheken" gemeint? Gibt es weitere Einschränkungen zu den TLS Zertifikaten? Gemeint ist eine nicht gematik-spezifische Prüfung ohne TI-Komponenten und ohne OCSP. Die Formulierung dient der Abgrenzung vom bisherigen Vorgehen. Beim Einsatz von TLS-Bibliotheken, wie z. B. OpenSSL, besteht keine Notwendigkeit, bis auf eine Root zu prüfen oder bestimmte Zertifikatsinhalte zu validieren. Hinsichtlich der TLS-Zertifikate gilt: Es sind keine EV-Zertifikate notwendig. Wichtig ist, dass die Zertifikatsherausgabe gemäß CAB-Forum erfolgt, und dass die CA Certificate Transparency unterstützt wird.
19	Kann die Intension der Anforderung A_23623 "Wahlfreiheit des Authentisierungsverfahren für TI-Anwendungen " genauer erläutert werden? Die IDP können Verfahren zur Nutzerauthentifizierung z.B. für die Administration des Nutzer-Accounts durch den Nutzer einrichten. Durch die Anforderung soll der Nutzer die Möglichkeit haben, solche Verfahren auch nur z.B. zu Administrationszwecken zu verwenden und damit nicht für den Zugriff auf TI-Anwendungen (E-Rezept) zu erlauben. Die Anforderung hat nicht das Ziel, dass der Nutzer ein bevorzugtes Authentifizierungsverfahren festlegen darf, sondern dass der Nutzer die Liste der vom sektoralen IDP angeboten Verfahren für TI-Anwendungen beschränken kann. Damit soll verhindert werden, dass ein verpflichtend eingerichtetes alternatives Verfahren immer auch den Zugriff auf TI-Anwendungen gewährt, ohne dass der Nutzer eine Wahl hat. Für die Festlegung muss der Nutzer nicht unbedingt die Verfahren im Einzelnen selbst bewerten können. Dem Nutzer muss lediglich die Liste der vom IDP unterstützen Authentifizierungsverfahren angezeigt werden, die zur Nutzerauthentifizierung für TI-Anwendungen zugelassen sind. Der Nutzer kann wählen (oder abwählen), welche dieser Verfahren zur Authentisierung für TI-Anwendungen benutzt werden dürfen.

20	Nach Anforderung "A_22939 - Widerspruch zur Weitergabe einzelner Scopes" soll der Nutzer die Möglichkeit haben, einzelne scopes abzuwählen. Auch auf das Risiko hin, dass der anfragende Fachdienst nicht ausgeführt werden kann. Diese Anforderung führt zum Akzeptanzverlust beim Nutzer. Ist es möglich die UX so zu gestalten, dass der Nutzer für den Fall, dass gar kein Anwendungsfall des Fachdienstes ausführbar ist, entweder allen scopes zustimmen oder sie ablehnen kann (z.B. bei ePA)? Es ist richtig, dass die Nutzerführung für den Fall, dass kein Anwendungsfall bei Abwahl einzelner scopes ausführbar ist, unpraktikabel ist. Um das Problem zu entschärfen, wurde die Anforderung A_22939 um einen Hinweis erweitert: "*Handelt es sich um eine dem sektoralen IDP bekannte Anwendung (z.B. durch direkte Registrierung eines Kassendienstes im Rahmen der A_23044) ist es zulässig dem Nutzer nur das Annehmen/Ablehnen aller geforderten scopes anzubieten.*"
21	Die Anforderung "A_23102 Weitere Verfahren zur Identifikation von Nutzern" benennt die Anforderungen an weitere zulässige Identifikationsverfahren neben eGK+PIN und online Ausweisfunktion, Wo kann die Liste der zulässigen Identifikationsverfahren eingesehen werden? Die Liste der zulässigen Identifikationsverfahren wird von der gematik gepflegt. Die aktuelle Version "Festlegung der zulässigen Identifikationsverfahren" steht im Fachportal der gematik unter https://fachportal.gematik.de/schnelleinstieg/smartcards-und-identitaeten-in-der-ti/identitaeten zum Download bereit.
22	Ist die Anforderung A_19041-01 so zu verstehen, dass der SigD erst nach dem ersten erfolgreichen Login des Nutzers über einen sektoralen IDP das X.509 Signaturzertifikat für diesen beantragen darf? Dies führt aufgrund der Dauer des Prozess dann dazu, dass der Nutzer zuerst in einen Timeout läuft und der SigD keine Möglichkeit hat eine direkte Information an den Nutzer zu senden weil der Prozess hinter dem ePA FdV gekapselt ist. Die Intention der Anforderung A_19041 war sicherzustellen, dass der Nutzer organisatorisch in den Prozess zum Erzeugen einer al.vi beim Signaturdienst einwilligt. Dies passierte im Rahmen der Identifikation des Nutzers, welche in der Regel an die Krankenkasse als Kartenherausgeber ausgelagert wurde. Nachdem nun die Identifikation und Authentisierung der Nutzer vom Signaturdienst auf den sektoralen IDP verlagert worden sind, wurde die Anforderung an die Authentisierung gekoppelt, was die erste Interaktion des SigD mit dem Nutzer darstellt. Dies sollte jedoch in keiner Weise die Prozesse verkomplizieren, sondern lediglich die vorherigen Festlegungen widerspiegeln. Daher ist es - abweichend von der Formulierung der Anforderung A_19041-01 - zulässig, weiterhin die Zustimmung des Nutzers zur Verwendung des SigD im Kontakt mit der Krankenkasse bzw. dem sektoralen IDP einzuholen. Der Kartenherausgeber kann dies durch das Auslösen der P_Create_Identity-Operation und initiale Bereitstellen der für den Zertifikatsabruf notwendigen Attribute signalisieren. Analog ist die Krankenkasse als Kartenherausgeber ebenfalls der Ansprechpartner des Versicherten für die Sperrung von Zertifikaten.
23	In den Anforderungen A_22235 und A_22236 ist vorgegeben, dass dem Versicherten Informationen bereitgestellt werden. Wie lange bzw. über welchen Zeitraum sollen diese Daten angezeigt bzw. aufbewahrt werden? Eine konkrete Vorgabe zur Aufbewahrungsfrist gibt es seitens gematik nicht. Mit Interpretation der zu protokollierenden Daten als "Protokolldaten" könnte man an §76 BDSG orientieren. Unsere Empfehlung ist daher eine dann Aufbewahrungsfrist von 1-2 Jahren.
24	Ist für die Erfüllung von A_21332 die serverseitige Prüfung ausreichend oder muss hier auch clientseitig (vom Authenticator-Modul) sichergestellt sein, dass nur die genannten Ciphersuiten unterstützt werden? Die Verbindung zwischen Authenticator-Modul und sektoralem IDP ist von der genannte Anforderung nicht betroffen. Das Authenticator-Modul ist keine getrennte Komponente für welche Interoperabilitätsvorgaben greifen. Für Verbindungen zwischen Authenticator-Modul und sektoralem IDP gilt konkret: *A_18986 - Fachdienst-interne TLS-Verbindungen* *Alle Produkttypen, die Übertragungen mittels TLS durchführen, die nur innerhalb ihres Produkttypen verlaufen (bspw. ePA-Aktensystem interne TLS-Verbindungen zwischen dem Zugangsgateway und der Komponente Authentisierung), KÖNNEN für diese TLS-Verbindungen neben den in GS-A_4384-* und ggf. A_17124-* festgelegten TLS-Vorgaben ebenfalls alle weiteren in [TR-02102-2] empfohlenen TLS-Versionen und TLS-Ciphersuiten mit den jeweiligen in [TR-02102-2] dafür aufgeführten Domainparametern (Kurven, Schlüssellängen etc.) verwenden.* Sofern serverseitig gewährleistet ist, dass nur Verbindungen unter Verwendung zulässiger Ciphersuiten aufgebaut werden und sofern Mechanismen zum Schutz vor MiM-Angriffen auf Seite des Clients etabliert sind, ist es zulässig, wenn dieser auch weitere Ciphersuiten unterstützen würde.

25	A_23700 sieht die Nutzung der System-PIN als Faktor zur Nutzerauthentifizierung vor. Gibt es Möglichkeiten die Komplexität von System-PIN bzw. System-Passwort zu ermitteln? Zumindest für Android Version >= 10 kann die Passwortkomplexität über die API geprüft werden. Mittels DevicePolicyManager.getPasswordComplexity() bekommt man eine ungefähre Einschätzung zur Komplexität des vom Nutzer vergebenen System-Lock (System-PIN/Passwort/Muster): ○ PASSWORD_COMPLEXITY_NONE --> kein Passwort ○ PASSWORD_COMPLEXITY_LOW --> Muster oder PIN mit Wiederholungen (z.B. 4444) bzw. geordneter Sequenze (z.B. 1234, 2467, ...) ○ PASSWORD_COMPLEXITY_MEDIUM --> PIN ohne Wiederholungen oder geordnete Sequenzen mit min. 4 Ziffern oder Passwort mit min. 4 Zeichen ○ PASSWORD_COMPLEXITY_HIGH --> PIN ohne Wiederholungen oder geordnete Sequenzen mit min. 8 Ziffern oder Passwort mit min. 6 Zeichen Für die Nutzung der API muss im Manifest die Berechtigung android.permission.REQUEST_PASSWORD_COMPLEXITY gesetzt sein Für den Abruf der Passwortkomplexität werden aktuell keine Device Admin Rechte benötigt. Die API liefert allerdings nur eine Information zum Ist-Stand. Veränderungen des System-Locks durch den Nutzer werden nicht automatisch gemeldet und sollten ggf. durch einen periodischen Abruf der API erfolgen. Achtung: Die Abfrage erfolgt in der Software und könnte durch App- oder Systemmanipulation falsche Werte zurückmelden. Deshalb sollten weitere Maßnahmen zur Sicherstellung der App- / Systemintegrität implementiert werden.
26	In der Spezifikation zum sektoralen IDP wird in „Tabelle 24: Body des Entity Statement des Fachdienstes“ definiert. Die Anforderung zum claim scope lässt mehrere Deutungen bezüglich des Formats zu: „scope1 scope2 scope3“ ; [scope1 scope2 scope3] ; [„scope1“ „scope2“ „scope3“] - Welche Formatvariante ist zu verwenden? Die derzeit veröffentlichte Spezifikation basiert auf OpenID Connect Federation 1.0 - draft 21. OpenID Connect Federation 1.0 - draft 29 ist im Kapitel 4.2 präziser hinsichtlich der möglichen Parameter für Relying Party und verweist zusätzlich auf *IANA.OAuth.Parameters].* • OpenID Connect Federation 1.0 - draft 21 *All parameters defined in Section 2 of OpenID Connect Dynamic Client Registration 1.0 [OpenID.Registration are allowed in a metadata statement.* *In addition, the parameters defined in Section 4 for OpenID Connect and OAuth2 entities and the following are added ...* • OpenID Connect Federation 1.0 - draft 29 *All parameters defined in Section 2 of OpenID Connect Dynamic Client Registration 1.0 [OpenID.Registration and Section 4.1 are applicable, as well as additional parameters registered in the IANA "OAuth Dynamic Client Registration Metadata" registry [IANA. OAuth.Parameters.* Das in der „Tabelle 24: Body des Entity Statement des Fachdienstes“ genannte Beispiel muss dem Format **"scope1 scope2 scope3"** entsprechen. (String mit durch Leerzeichen getrennten Bezeichnungen ohne Klammern.) Wir werden bei der nächsten Spezifikationsanpassung unsere Beispiele entsprechend anpassen und ggf. zusätzlich auf die referenzierten Standards verweisen.
27	Wie bekommt ein Fachdienst das Pseudonym eines Versicherten? Um das Pseudonym eines Versicherten zu erhalten, muss der Fachdienst im Pushed Authorization Request den scope "openid" anfordern. Nach erfolgreicher Nutzerauthentisierung ist im vom sektoralen IDP ausgestellten ID-Token der claim "sub" mit einer pseudonymen ID des Versicherten gefüllt. Das Pseudonym muss spezifisch je Nutzer, Fachdienst und IDP sein. Damit das erreicht wird, muss ein Fachdienst die pseudonyme ID des Versicherten in Kombination mit dem iss des ausstellenden IDP verwenden. (siehe Anforderung A_23036 und A_23035) Der scope "openid" ist immer Bestandteil der Anfrage eines Fachdienstes, deshalb wird jeder Fachdienst auch immer mindestens auf diesen scope registriert.

28	Wie bekommt ein Fachdienst die KVNR eines Versicherten? Damit ein Fachdienst überhaupt die KVNR eines Versicherten im vom sektoralen IDP ausgestellten ID-Token erhalten darf, muss dieser beim Federation Master für den scope "urn:telematik:versicherter" registriert sein. Der Fachdienst muss nun im Pushed Authorization Request an den sektoralen IDP den scope "urn:telematik:versicherter" anfordern. Dieser scope enthält u.a. den claim "urn:telematik:claims:id". Im vom sektoralen IDP ausgestellten ID-Token ist der Wert des claims mit der KVNR des Versicherten belegt.
29	In der Anforderung A_22306 ist formuliert, "..... Der Anbieter des sektoralen Identity Provider MUSS auf der unter redirect_uri des Authenticator-Moduls erreichbaren Webseite darstellen ....". Gemäß der Anforderung A_22744 muss der IDP für den Auth-Endpunkt ein WebFrontend zur Verfügung stellen. Die Information wird allerdings nicht über eine redirect_uri transportiert. Wie ist die Anforderung A_22306 zu verstehen? Die Anforderung A_22306 ist nicht korrekt formuliert. Erfüllt werden soll diese Bedingung: *"Der Anbieter des sektoralen Identity Provider MUSS auf dem WebFrontend für den Auth-Endpunkt (siehe A_22744) darstellen, aus welcher Quelle das jeweilige Authenticator-Modul des sektoralen Identity Provider zu beziehen ist, auf welchen Geräten/Plattformen es installiert werden kann und welche Voraussetzungen für die Verwendung zur Authentifizierung zu erfüllen sind (z. B. erforderliche Registrierungsprozeduren beim Anbieter des sektoralen Identity Provider)."* Die Formulierung wird mit der nächsten Auslieferung korrigiert.
30	Bei der Erstellung eines Sicherheitsgutachtens für ein Produkt Sektoraler Identity Provider nach gemProdT_IDP-Sek_PTV_2.0.3-0 ist die Anforderung A_21332 - E-Rezept: TLS-Vorgaben aufgefallen. Während alle anderen Anforderungen sich auf den Produktlebenszyklus bzw. die Entwicklungsprozesse beziehen, geht es in der A_21332 um Vorgaben zur produktseitigen Unterstützung von TLS Ciphersuiten und bestimmten elliptischen Kurven. Ist die Anforderung evtl. fälschlicherweise dem Sicherheitsgutachten zugeordnet worden und gehört eigentlich ins Produktgutachten? Die Anforderung A_21332 ist tatsächlich fälschlicher Weise dem Sicherheitsgutachten zugeordnet. Die Zuordnung zur Prüfung im Rahmen eines "Produktgutachten" wäre korrekt. Die Korrektur wird mit dem nächstmöglichen Release ausgeliefert.
31	*[A_22844 - Transportverschlüsselte Übertragung von Daten mit Fachdiensten]* fordert mTLS in der Kommunikation mit Fachdiensten. Im Falle, dass die Prüfungen ergeben, dass mTLS erforderlich ist (z.B. Auslösung PAR durch Fachdienst), jedoch kein Zertifikat vom Client übermittelt wurde: • **MUSS** der IdP-Sek die Verbindung zwingend auf TLS-Protokoll-Ebene terminieren und damit einhergehend in die Produkttyp-übergreifenden Vorgaben aus *[GS-A_5542 - TLS-Verbindungen (fatal Alert bei Abbrüchen)]* laufen • *o d e r* **DARF** der IdP-Sek per HTTP-Protokoll einen 401 Forbidden-Status mit ergänzendem Fehler-Payload (z.B. JSON) liefern? GS-A_5542 greift immer dann wenn die TLS Verbindung nicht etabliert werden konnte. Zu diesem Zeitpunkt besteht noch keine HTTP Verbindung. Es hängt davon ab, wie restriktiv der Server, welcher das Clientzertifikat anfordert, implementiert oder konfiguriert ist. Das bedeutet, dass ein Server es akzeptieren kann, wenn er kein Clientzertifikat erhält. Der Verbindungsaufbau wird dann nicht zwangsläufig abgebrochen. In diesem Fall ist der Verbindungsaufbau (nur) TLS. Dann kommt es zum Datenaustausch auf Anwendungsebene. In diesem Fall kann der sektorale IDP kann entsprechend RFC8705 ein HTTP-Error werfen. Andernfalls bricht der Server den TLS-Aufbau ab und muss nach GS-A_5542 mit einem "fatal Allert" reagieren. Diese Anforderung einer bereits etablierten TLS-Verbindung wird durch RFC 8705 Sektion-2 klar formuliert: *"In order to utilize TLS for OAuth client authentication, the TLS connection between the client and the authorization server MUST have been established or re-established with mutual-TLS X.509 certificate authentication (i.e., the client Certificate and CertificateVerify messages are sent during the TLS handshake)."* War der TLS-handshake erfolgreich, kann der sektorale IDP die Konfiguration des Clients aus dessen Entity Statement gegen das Zertifikat aus dem TLS-handshake prüfen. Wenn der TLS-Aufbau funktioniert hat aber dieses Zertifikat dann auf Anwendungsebene (Open-ID) nicht vorhanden ist oder als nicht vertrauenswürdig für diese Client-ID erkannt wird, dann muss der sektorale IDP den Fachdienst als "unbekannten Client" behandeln. In diesem Fall gilt *A_22649 - Anfragen unbekannter Clients* *Der Produkttyp sektoraler IDP MUSS Pushed Authorization Request von Clients mit dem http-Statuscode 401 (Unauthorized) ablehnen, wenn diese nicht in der Föderation oder direkt beim sektoralen IDP registriert sind. Ist der Fachdienst dem sektorale IDP nicht bekannt, so stößt dieser intern die automatische Registrierung (https://openid.net/specs/openid-connect-federation-1_0.html#section-10.1.1.1.1) an damit nachfolgende Anfragen angenommen werden können.* Diese Anforderung entspricht der Regelung im Standard RFC 8705 und RFC6749 Section-5.2 "invalid_client".

	Fragen & Antworten zur Zulassung oder Registrierung von Fachdiensten und sektoralen Identity Providern
32	Welche Anforderungen gelten für die Zulassung eines IDPs? Die Anforderungen für die Produktzulassung eines sektoralen Identity Provider sind im aktuellen Produkttypsteckbrief unter dem Kapitel 3 „Normative Festlegungen“ zu finden. Hier sind alle normativen Festlegungen, die für die Herstellung und den Betrieb des Produktes notwendig sind, aufgelistet. Im Falle des Sektoralen Identity Provider zählen hierzu: 1. Funktionale Eignung a. Produkttest/Produktübergreifender Test b. Herstellererklärung funktionale Eignung 2. Sicherheitstechnische Eignung a. Herstellererklärung sicherheitstechnische Eignung b. Sicherheitsgutachten c. Produktgutachten Darüber hinaus beachten Sie bitte die zugehörige Verfahrensbeschreibung im Fachportal https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen.

33

Bei der Registrierung eines sektoralen IDP sollen folgende Werte angegeben werden:

Öffentliche/r Schlüssel für JWT - Bitte fügen Sie eine Datei im .pem-Format als Anlage hinzu. Der Dateiname dieser Datei muss mit dem Präfix „jwt_“ beginnen. Der Inhalt der PEM-Datei: Ein oder mehrere öffentliche Schlüssel inklusive Angabe entsprechender key identifier (kid(s)). Den/die kid(s) bitte wie im Beispiel in Doppel-Hochkommata " " setzen. Öffentliche/r Schlüssel für TLS - Bitte fügen Sie eine weitere Datei im .pem-Format als Anlage hinzu. Der Dateiname dieser Datei muss mit dem Präfix „tls_“ beginnen. Inhalt der PEM-Datei: Ein oder mehrere öffentliche Schlüssel inklusive Angabe der Domain, jeweils als Tupel. Die Domain bitte wie im Beispiel in Doppel-Hochkommata " " setzen.

Welche Schlüssel sind hier mit „Öffentliche Schlüssel für JWT/TLS“ gemeint?

Für sektorale IDP gilt:

"Öffentliche/r Schlüssel für JWT"

Das Entity Statement eines sektoralen IDP muss als signiertes JWT abrufbar sein (*siehe A_22643 - Entity Statement des sektoralen IDP*). Zur Prüfung der Signatur des JWT ist ein öffentlicher Schlüssel notwendig.
Dieser öffentliche Schlüssel, mit dem die Signatur geprüft werden kann, ist der "Öffentliche/r Schlüssel für JWT", welcher bei der Registrierung des sektoralen IDP anzugeben ist.

"Öffentliche/r Schlüssel für TLS"

Die HTTP(S)-Verbindungen zwischen Fachdiensten und sektoralen IDPs müssen als mTLS-Verbindungen realisiert werden (*siehe A_22864 - Umsetzung von Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)*).

Diese öffentlichen Schlüssel für die Transportverschlüsselung ist der "Öffentliche/r Schlüssel für TLS", welcher bei der Registrierung des sektoralen IDP anzugeben ist.

Allgemein gilt für die Schlüsselerzeugung die Anforderung:

A_22868 - Private Schlüssel im HSM

Der sektorale IDP MUSS folgende private Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

- *die Schlüssel zur Signatur von Token und Entity Statements*
- *die Schlüssel der TLS-Zertifikate für die sichere Verbindung zum Verarbeitungskontext*

Die Prüftiefe des HSM MUSS dabei den in [A_22829] angegebenen Standards entsprechen.<=

Für Fachdienste gilt:

Für die Registrierung von Fachdiensten gilt:

A_23045 - Registrierung des Fachdienstes
Anbieter von Fachdiensten MÜSSEN bei der Registrierung ihrer Authorization-Server am Federation Master die von ihnen erwarteten Attribute in scopes (siehe Abschnitt ML-128467) beschreiben und dem Federation Master zur Verfügung stellen. Die Registrierung MUSS ebenso die absolute URI des Fachdienstes im Internet umfassen (seine Client-ID) ***sowie dessen Signaturschlüssel für das Entity_Statement****.*

Um den Vertrauensraum sicherzustellen, müssen Änderungen dieser Schlüssel auch nach der Registrierung im produktiven Betrieb immer über den organisatorischen Prozess dem Federation Master übermittelt werden.

Fragen & Antworten zu Test und Betrieb sektoraler Identity Provider

34

Ist es aus Sicht der gematik zulässig, dass die sektoralen IDPs verschiedener logischer Mandanten in einem identischen Rechenzentrum durch den gleichen Betreiber betrieben werden können?

Aus Sicht der gematik ist das zulässig sofern für alle Mandanten gesichert ist dass deren sektoraler IDP den zugrunde liegenden Spezifikationen genügen.

35	Ist es aus Sicht der gematik zulässig, dass eine Trennung pro Nutzer erfolgt und somit zweitranging ist, ob dieser zu Krankenkasse 1 oder Krankenkasse 2 gehört? Jede Kasse wird als eigener IDP mit eigenen Endpunkten und Entity Statements geführt. Ein Betreiber kann dahinter aber denselben Dienst stehen haben und die Kassen als Mandanten pflegen. Auf einem physischen Multi-Tenant Sek-IDP mit einer Anbieter- und Produktzulassung der gematik für das System, den Betrieb und die bewerteten Identifizierungs- und Authentifikations-Mechanismen können beliebig viele logische Sek-IDP-Instanzen aufgebaut werden. Die kommerzielle Abbildung, wem gehört die physische Instanz und mögliche Modelle für eine Rücklizensierung / Weiterveräußerung des Sek-IDP-Ansatzes, sind von der Abbildung des Sek-IDP für die gematik nicht relevant. Die gematik wendet sich immer an den Inhaber der Produkt - / Anbieterzulassung des (physischen) Sek-IDP und bespricht mit diesem alle Fragen rund um die logischen Instanzen der Krankenkassen auf dieser physischen Instanz. Es besteht eine Informationsverpflichtung über Mandanten des Anbieters sektoraler IDP. Die gematik wird über die aktuellen Mandanten des jeweiligen Anbieters informiert. Wenn der sektorale IDP eines weiteren Mandanten über bereits zugelassene Prozessabläufe und Funktionalitäten (die z. B. bereits für bestehende Mandanten genutzt werden) abgebildet werden kann (z. B. gleiche Art der Anbindung an Kassensysteme, gleicher Prozess zur Zuweisung von Schlüsselmaterial, gleiche oder eine Unterauswahl von Authentisierungsmethoden), dann benötigt der Anbieter keine neue Produkt- oder Anbieterzulassung, um den neuen Mandanten auf dem System abzubilden. Delta-Gutachten und eine Delta-Zulassung werden nur im Falle einer Erweiterung des Funktionsumfangs, Veränderungen an den Schnittstellen zu den Systemen der Mandanten, Veränderungen an den Sicherheitsvoraussetzungen und insbesondere bei zusätzlichen Authentisierungsverfahren erforderlich. Veränderungen im Bereich der Darstellung der Funktionen für den Endnutzer (UI, CI, CD) sind irrelevant, solange sie nicht Vorgaben unterlaufen. Sollte ein logischer Mandant (KK) nur eine Auswahl aus dem Set der in der Anbieter – und Produktzulassung freigegebenen Ident- / Authent-Verfahren und genehmigten Prozesse benutzen, so ist kein erneutes Sicherheitsgutachten bzw. eine erneute Zulassung oder Delta-Zulassung bei der gematik erforderlich. Sollte ein logischer Mandant (KK) im Vergleich zum Set der in der Anbieter – und Produktzulassung freigegebenen Ident- / Authent-Verfahren und genehmigten Prozesse weitere oder andere Ident- / Authent-Verfahren und / oder Prozesse benutzen, so ist in dem Fall ein erneutes (Delta-) Anbieter- und Produkt-Sicherheitsgutachten bzw. eine Delta-Zulassung bei der gematik erforderlich. Die Aufnahme eines neuen Mandanten erfolgt mittels Anzeige / Registrierung des neuen logischen Tenant gemäß Anforderungen gematik-Sek-IDP-Spezifikation (mit zugehörigen Prozessen, Zuweisung Kennung und Schlüsselmaterial durch die gematik). Die logischen Mandanten können alle Ressourcen des physischen Systems (Storage, Server, HSMs) in einem shared Modus nutzen. Eine Abbildung pro Nutzer n=1 ist irrelevant. Es erfolgt immer die Zuordnung auf der Ebene der logischen Mandanten (Krankenkassen) als Summe der Nutzer pro Krankenkasse. Dabei müssen die Mandanten auf allen Ebenen logisch bzw. über Mechanismen der Software getrennt werden, so dass alle Prozesse eines Mandanten (z. B. Registrierung und De-Registrierung des Mandanten, Konfiguration des mandantenspezifischen Kontextes, DNS-Einträge) ohne Einfluss auf andere Mandanten ablaufen bzw. durchgeführt werden können. Konkret bedeutet dies, dass je Mandant dedizierte Enklaven gestartet, dediziertes Schlüsselmaterial - in unabhängig vollziehbaren Zeremonien - registriert und dedizierte Storage-Bereiche genutzt werden müssen. An den IDP eines Mandanten gerichtete Requests werden durch das System an eine dem Mandanten zugeordnete Enklave geroutet, die sich mittels des nur ihr zugänglichen Schlüsselmaterials als Service mit der dem Mandanten zugeordneten Identität ausweist. Die Requests bzw. Sessions verschiedener Nutzer werden innerhalb der Enklave des IDP-Mandanten z. B. auf Thread-Ebene isoliert. Die Bewertung der sicherheitstechnischen Qualität dieser nutzerbezogenen Trennung im Verarbeitungskontext ist Gegenstand des Produktgutachtens.
36	Gibt es keine Anforderungen hinsichtlich der Validierungsidentitäten? Zur Überprüfung der Erreichbarkeit des sektoralen IDP werden durch die gematik regelmäßig invalide Requests an diese Schnittstellen gemäß Entity Statement (siehe Tabelle: "Body Entity Statement des sektoralen IDP") gestellt: • pushed_authorization_request_endpoint • token_endpoint Als Ergebnis der Request wird ein Fehlercode gemäß [OpenID Connect Federation 1.0#rfc.section.7.5] erwartet. Testidentitäten müssen demnach in der produktiven Umgebung nicht bereitgestellt werden. Es gibt darüber hinaus keine Anforderungen an Validierungsidentitäten. Selbstverständlich können sektorale IDP Validierungsidentitäten implementieren, wenn sie diese zur Sicherstellung ihrer Funktionalität benötigen. Normative Vorgaben für Validierungsidentitäten gibt es jedoch nicht. Anbietern steht es frei sich, falls benötigt, Validierungsaktenkonten für eigene Zwecke anzulegen welche idealerweise den Einigungen zur ePA dahingehend folgen, dass nur Versichertennummern aus dem von der gematik freigegebenen Nummernkreis [gem. gemSpec_PK_eGK] verwendet werden. Entsprechend Card-G2-A_3820 MUSS die Versichertennummer X0000nnnnP, mit nnnn aus der Menge {0001 .. 5000} und P = Prüfziffer entsprechen.

37	In der AF_10100 der gemSpec_IDP_FedMaster wird verlangt, dass der Anwender (selbst) eine Auswahl des für ihn zuständigen IDP-Providers in seiner App treffen muss. Die Gesamtliste aller sektoralen Provider wird dazu dem Client vom Federation Master übergeben. Die Anforderung formuliert, dass es der Anwender sein MUSS, der die Auswahl trifft. Eine automatische Auswahl durch die App ist hierbei nicht erwähnt. Ist eine solche verboten? Die Mechanismen der Föderation decken kassenübergreifende Anwendungsfälle ab. Für Anwendungen, die nicht übergreifend durch mehrere IDPs unterstützt werden sollen, ist es ausreichend diese direkt bei den jeweiligen IDPs zu registrieren. Die Föderation bietet hier keinen Mehrwert da beide Kommunikationspartner sich ohnehin kennen und vertrauen. (Siehe den letzten Absatz Kapitel 2.1 in gemSpec_IDP_Sek). Direkte 1:1 Beziehungen wie etwa auch zum Signaturdienst im Kontext der ePA werden nicht über die Föderation behandelt, sondern über eine direkte Anbindung an den sektoralen IDP der jeweiligen Kasse. Der IDP muss diese lediglich entsprechend A_23021 differenzieren. Im von Ihnen skizzierten Anwendungsfall ist der Anwendung (App) die Kasse bzw. der zugehörige IDP des Nutzers nicht bekannt. Für diesen Fall ist beschrieben, was Federation Master und Fachdienst bereitstellen müssen, um dem Nutzer eine Auswahl zu ermöglichen. Der Nutzer muss dann eine Auswahl treffen, damit der Authentifizierungsablauf überhaupt starten kann. Wenn der Fachdienst (bzw. die App) die Zugehörigkeit des Nutzers zu einer Krankenkasse oder -versicherung und damit zu einem konkreten IDP kennt (z.B. weil in einer vorherigen Nutzung bereits eine Zuordnung stattgefunden hat), dann ist die Auswahl durch den Nutzer nicht notwendig. Der Anwendungsfall AF_10100 muss also nur ausgeführt werden, wenn der Fachdienst die Zuordnung des Anwenders zu seinem IDP nicht kennt. Dazu Zeile „Ablauf“ in der Tabelle zum AF_10100: • Im Ablauf der Nutzung eines Fachdienstes (siehe Abbildung - Aktivitätsdiagramm "Auswahl sektoraler Identity Provider") findet eine Verzweigung zum Federation Master in dem Fall statt, wenn der Fachdienst die Zuordnung des Anwenders zu seinem IDP nicht kennt.
38	TLS-Vorgaben sind im Produktsteckbrief sowohl dem Test als auch dem Produktgutachten zugewiesen. Ist das korrekt? Und falls ja, welche Aspekte der Anforderung sollen per Test und welche per Produktgutachten nachgewiesen werden? Die Anforderung A_21332 ist nicht neu im Kontext der sektoralen IDP, sondern besteht im Kontext E-Rezept schon seit Anfang 2021 mit den beiden zugeordneten Prüfverfahren. Seitens Hersteller kann alles getestet werden. Der Gutachter kann prüfen, ob Ciphersuiten unterstützt werden, die nicht unter Punkt (1) der Anforderung und nicht in TR-02102-2, Abschnitt 3.3.1 Tabelle 1 aufgeführt sind.
39	Sind Nachweise gemäß C5 ebenfalls zur Erfüllung Anforderung GS-A_3772-01 geeignet? Die Vorgaben zum Notfallmanagement in C5 decken generell dieselben Bereiche wie der BSI-Standard 100-4 ab. Entsprechend der Kreuzreferenztabelle des BSI zur Bewertung des C5 ist dessen Umsetzung mindestens Gleichwertig und damit akzeptabel.

40	Die Anforderung A_22225 erscheint sprachlich dahingehend nicht eindeutig, auf was sich der Satzteil „die diese Anwendung nutzen“ bezieht. Die Gesamtnutzerzahl als Anzahl aller Versicherten (gesetzlich + privat), die diese Anwendung nutzen änderte sich laufend und erforderte Kenntnis über die Nutzerzahlen anderer Anbieter von sektoralen IDPs bei den Kostenträgern. Oder bezieht sich „die diese Anwendung nutzen“ nur auf die Anzahl der LE und LEO? Die Einschränkung: „die diese Anwendung nutzen.“ bezieht sich auf die Einordnung zum Nutzerkreis. Das heißt, beim „Anbieter sektoraler IDP KTR“ sind die Nutzer die ***Versicherten***. Versicherte = Gesamtnutzerzahl = 72,3 Mio gesetzlich Vers. + 8,8 Mio privat Vers. = **81,1 Mio** Die konkret für die Anteilsbetrachtung relevanten Nutzer sind die bei allen Mandanten (=Kassen) des Anbieters in Summe vorhandenen Versicherten. Das ist unabhängig davon, ob diese Versicherten den IDP „aktiv nutzen“, sondern dass sie den IDP potentiell nutzen könnten. Der Sinn der anteiligen Performancevorgabe ist, dass alle Anbieter zusammen die geforderte Last (hier 450 Requests pro Sekunde) bereitstellen - aufgeteilt jeweils zur Anzahl der bei ihren Mandanten zugehörigen Versicherten. Zusätzlich ist noch ein Sockel (10 Requests pro Sekunde) eingebaut, der für eine Grundlast und für Systemabfragen notwendig ist. Für die Annahme „Eigene Kunden des Anbieters = derzeit 8 Mio Versicherte Krankenkasse xy“ gilt somit: Für den Anbieter sektoraler IDP KTR, bei welchem alle Versicherten der Krankenkasse xy Mandant sind, würde das bedeuten: MA = 8/81,7 = 0,098 0,10 Die derzeitig vorgeschriebene Last beträgt hier dann: 10 + 450x0,10 = 55 Hinweis: Einem Anbieter wird eine Adaptierung im Zuge eines Aufbaus oder Abbaus der Zahlen der Versicherten ihrer Mandanten eigenverantwortlich zugetraut. Anlassbezogen kann bei auftretenden Performance-Problemen, die in den Rohdaten jederzeit nachvollzogen werden können, die Performancevorgeben überprüft werden. Darüber hinaus möchten die Kassen für ihre eigenen Anwendungen, die nicht in diesen Performance-Vorgaben enthalten sind, dieselbe von ihnen bereitgestellte Infrastruktur nutzen und sind daher intrinsisch motiviert, eine höhere Performance im System vorzusehen. Sollte sich - insbesondere bei einer größer werdenden Anzahl von Anwendungen in der TI - die Performancevorgabe erhöhen, wird das in einem Folgerelease für alle Anbieter bekanntgegeben. Eine solche Skalierung ist grundsätzlich immer zu erwarten.
41	In A_23236-04 wird die Angabe des Registrierungsverfahrens für die Bestandsinformationen gefordert. Im Zeitablauf kann der Nutzer unterschiedliche Registrierungsverfahren nutzen. Wir ermöglichen dem Nutzer außerdem, weitere Ident-Verfahren zu hinterlegen nach der initialen Registrierung. Wie soll die Zählung gehandhabt werden, wenn verschiedene Verfahren genutzt werden? Es gibt einen Grund, warum der Versicherte seine Registrierung erneuert bzw. eine erneute Registrierung durchführt. Die Grundannahme ist, dass die alte (bisherige) Registrierung dann hinfällig ist und der IDP aufgrund der neuen Registrierung die Nutzung ermöglicht. Deshalb ist die alte Registrierungsinformation bei einer erfolgreichen neuen Registrierung zu entfernen und nur die letzte in den Bestandsdaten zu reporten. Eine Mehrfachregistrierung mit unterschiedlichen Verfahren gleichzeitig ist weder sinnvoll noch vorgesehen.
42	Die Anforderung “A_22504 - Performance - Rohdaten - Spezifika IDP - Feldtrennzeichen im Useragent (Rohdatenerfassung v.02)” in gemSpec_Perf_2.31 bezieht sich auf “Useragent-Wert”. Ist hier der Useragent-Wert aus “A_22016-01 - Performance - Rohdaten - Spezifika IDP - Message (Rohdatenerfassung v.02)” (nicht im Produktsteckbrief 2.0.3 enthalten) gemeint? Bei der Überprüfung des Kontextes der Anforderung A_22504 haben wir festgestellt, dass diese Anforderung für die aktuelle Produktversion zum sektoralen IDP nicht mehr relevant ist und ignoriert werden kann. Wir korrigieren die Zuweisung der Anforderung zum sektoralen IDP, so dass sie in der nächsten Veröffentlichung des Produktsteckbriefes nicht mehr enthalten ist.
	Fragen & Antworten zu Gesetzesgrundlagen & Richtlinien
43	Wie ist der Status zur Gesetzesgrundlage "al.vi" nach Ablauf der Duldung des BfDI für das Sicherheitsniveau "substanziell" Ende 2023? Unsere Rechtsabteilung teilt die Auffassung, dass der Zugriff auf die ePA gemäß § 336 Abs. 2 SGB V getrennt von der einer elektronischen Identität zu sehen ist und demnach parallel dazu angeboten werden kann. Beide Zugriffsmöglichkeiten basieren auf unterschiedlichen gesetzlichen Grundlagen. Jedoch gelten damit dann auch die Vorgaben und Freiheiten für die eID nicht auch für diesen Weg, sodass man nach Ablauf der Duldung des BfDI für eine Absenkung des Schutzniveau nur noch über eGK bzw. nPA als zulässige Authentisierungsmittel sprechen würde.

44	Was passiert im Migrationsfall (Ablösung der al.vi) mit bestehenden Gerätebindungen. Müssen diese neu angelegt werden? Startet ihre Gültigkeitsdauer mit dem Zeitpunkt der Migration? Oder startet ihre Gültigkeitsdauer mit dem Zeitpunkt, zu dem die Gerätebindung ursprünglich angelegt wurde? Im Migrationsfall startet die Gültigkeitsdauer einer existierenden Gerätebindung entsprechend A_22750-01 mit dem Zeitpunkt zu dem die Gerätebindung ursprünglich angelegt wurde. Alternativ muss eine neue Gerätebindung nach der Migration angelegt werden.
45	Was passiert im Migrationsfall (Ablösung der al.vi) mit bestehenden Identifikationen. Unter welchen Umständen müssen Nutzer erneut eine Identifikation durchlaufen? Wenn ein Nutzer mit einem Verfahren identifiziert wurde, das gemäß der veröffentlichten Liste der zulässigen Identifikationsverfahren ("Festlegung der zulässigen Identifikationsverfahren" (https://fachportal.gematik.de/schnelleinstieg/smartcards-und-identitaeten-in-der-ti/identitaeten) verwendet werden darf, so ist dieser nicht erneut zu identifizieren, bevor er seine Gesundheits-ID nutzen darf.
46	Wurde mit der Veröffentlichung der aktuellen Liste “Festlegung der gematik bzgl. der Zulässigkeit von Identifikationsverfahren für das Level of Assurance (LoA) "gematik-ehealth-loa-high“ beabsichtigt, die Möglichkeiten der sicheren PIN-Zustellung gem. § 336 Abs. 5 Nr. 1 und Nr. 4 auszuschließen? Gemeint ist hier insbesondere die Streichung des PostIdent-Zustellungsverfahrens aus der Liste. Wir gehen dbzgl. davon aus, dass die eGK-PIN in einem Verfahren mit einer Identifizierung gem. "gematik-ehealth-loa-high" ausgegeben werden muss, um für den Sektoralen IDP als Authentifizierungsmittel in dem entsprechenden Niveau zu dienen. Das Postfilial-Ident sieht derzeit weder eine Briefzustellung, noch einen mit der Identifizierung gleichzeitigen Nachweis des Besitzes der eGK vor. Die Zustellung der PIN mit PostIdent Zustellung ist valide. Es ist nur kein zulässiges Verfahren um als alleiniges Ident der Gesundheits-ID verwendet zu werden. Demnach können auf dem beschriebenen Weg eGK und PIN ausgeliefert und dann diese Karte als Identmedium für den IDP verwendet werden. Es ist also nicht so, dass die eGK und PIN ebenfalls zwingend in einem Verfahren mit einer Identifizierung gemäß "gematik-ehealth-loa-high" verknüpft werden müssen. Dort gelten die bestehenden Festlegungen und Prozesse.
	Fragen & Antworten zu angewandten Standards
47	Nach Open ID Connect Spec müsste es eigentlich so sein, dass bei einer Anfrage mit acr_values das erreichte LoA in acr zurück geliefert wird, solange nicht über Essential Claim Values ein bestimmtes LoA erzwungen wird. Ist es geplant, die gematik-Spezifikation dahingehend anzupassen, die Essential Claims mit anzufragen, damit der IDP auch nach Spezifikation mit einem Fehler antworten darf? In der Vorab-Klärung zur Spezifikationserstellung wurde das Anfragen einzelner claims zugunsten der scopes abgelehnt. Daher wurde der Weg über die *acr_values* und den *acr*-Rückgabewert gewählt. Der sektorale IDP lehnt den Request eines Fachdienstes nicht zwingend ab, wenn das *acr_values* nicht in ausreichender Güte erfüllt werden kann, sondern gibt dem Fachdienst im claim *acr* des ID-Token das Vertrauensniveau des durchgeführten Authentisierungsverfahren zurück (siehe Anforderung A_ 23129). Welches Authentifizierungsverfahren durchgeführt wurde, wird im claim *amr* im ID-Token dem Fachdienst zurückgegeben. Der Fachdienst muss prüfen, ob das im ID-Token im Feld *acr* gelistete Vertrauensniveau der durchgeführten Authentisierung für den Zugriff auf ihre Fachdaten ausreicht. So wäre es auch möglich, dass der Fachdienst bei einer weniger starken Authentisierung verschiedene Operationen nicht anbietet bzw. bei deren Aufruf eine erneute Authentisierungsanfrage stellt.
48	Die Spezifikationen für die TI-Föderation basieren auf OpenID Connect Federation 1.0 - draft 21. Inzwischen gibt es OpenID Federation 1.0 - draft 32 (Stand 12/2023). Ist angedacht, die Spezifikationen an den aktuellen Standard anzugleichen? Aktuell ist die Änderungshäufigkeit der veröffentlichten Versionen des OpenID Connect Federation Standard noch sehr hoch. Wir beobachten die Entwicklung und werden für die TI-Föderation relevante Änderungen in die Spezifikationen aufnehmen. Eine komplette Anhebung möchten wir durchführen, wenn der Standard einen finalen Status erreicht hat.