FAQ

	Frage	Antwort
1. Fragen zur Testumgebung der GesundheitsID bzw. TI-Föderation:		
1.1	Was kann ich jetzt schon testen und welche Voraussetzungen müssen dafür erfüllt sein?	Aktueller Testumfang und die notwendigen Voraussetzungen sind in der IDP Wissensdatenbank/Fachdienste Test-Umgebungen beschrieben.
1.2	Ich kann nicht auf die Referenzimplementierung des sektoralen IDPs der gematik über das Internet zugreifen. Woran könnte das liegen?	Zugriff auf unseren IDP ist nur möglich, wenn Ihre outbound IP auf unserer Allowlist steht oder Sie unseren X-Auth-Header verwenden. Einfach eine Mail an uns schicken und entweder Ihre outbound IP angeben oder den X-Auth-Header erfragen. **Bezüglich der App-Veröffentlichung:** Wir arbeiten mit Hochdruck daran und hoffen, Ihnen die Anwendung bis Ende November zur Verfügung stellen zu können. Für weiterführende Informationen verweisen wir zusätzlich auf die der IDP Wissensdatenbank/Fachdienste Test-Umgebungen.
1.3	Wie sieht es bei der GesundheitsID aus? Kann die Referenzimplementierung auch ohne SMC-B erfolgen? Oder müssen Hersteller auch hier erst mit der Implementierung warten, bis sie erfolgreich gelistet sind?	Sie benötigen für die Integration der GesundheitsID keine SMC-B. Auf die Testumgebung zur Integration der GesundheitsID dürfen auch Anwendungen zugreifen, die noch nicht als DiGA gelistet sind. Eine Registrierung in der Produktivumgebung erfolgt allerdings erst nach der Listung. Für weiterführende Informationen zur Testumgebung verweisen wir zusätzlich auf die IDP Wissensdatenbank/Fachdienste Test-Umgebungen.
1.4	Wie lange dauert es üblicherweise, bis mein Registrierungsantrag bearbeitet wird?	Eine reguläre Registrierung nimmt durchschnittlich 5 Arbeitstage in Anspruch. Bei fehlerhaften Registrierungsdaten muss eine Klärung mit Ihnen stattfinden, weshalb sich die Bearbeitungszeit dementsprechend verlängert. Sobald der Dienstleister die erfolgte Registrierung bestätigt, erhalten Sie die Information umgehend.
1.5	Wie und wo erfolgt die Bereitstellung eines Entity Statements?	Ein Entity Statement wird unter einer URL bereitgestellt, die vom Hersteller der DiGA gehostet wird. Diese URL korrespondiert mit der client_id der Anwendung.
1.6	Braucht man für Test und Prod unterschiedliche client_ids?	Die Registrierung für die Testumgebung sind nicht dauerhaft. Testumgebungen und Produktivumgebungen dürfen nicht vermischt werden. Es wäre möglich den Endpunkt erstmal für die Testumgebung bereitzustellen, dann das Testsystem abbaut und die Endpunkte für Produktivumgebung nutzen. Abbau Testumgebung bedeutet auch Deregistrierung der DiGA am Federation Master.
1.7	Ist es ausreichend, wenn eine von mehreren angebotenen DiGAs die Testumgebung durchläuft?	Im Allgemeinen nein. Jede DiGA muss individuell geprüft und bestätigt werden, da unterschiedliche Entity Statements notwendig sind. Dies gewährleistet eine korrekte Registrierung jeder einzelnen DiGA. Wendet Euch mit ganz konkreten Spezialfällen gern nochmal an uns.
1.8	Was bedeutet der Fehler "invalid_request (GSI Runtime Exception: missing claim: openid_relying_party)" beim PAR?	Dieser Fehler bedeutet, dass der gematik sektorale Identitätsprovider Probleme bei der Verarbeitung des Entity Statement des Fachdienstes hat.
1,9	Was sind die nächsten Schritte, die ich befolgen muss, nachdem ich die Integration der GesundheitsID erfolgreich getestet habe?	Bitte sehen Sie sich den Leitfaden unter "Anmeldung an der DiGA mit der GesundheitsID" - "Umsetzung des Anwendungsfalls" an.
1.10	Gibt es eine Referenzimplementierung für eine Fachanwendung?	Unsere Minimalimplementation des Authorization Server eines Fachdienstes ist auf github: https://github.com/gematik/app-gemRAS Hier kann man sich angucken, wie wir den Flow in Java umgesetzt haben und hilft vielleicht dabei die API zu verstehen. Lässt sich aber vermutlich nur sehr beschränkt in eigenen Projekten nachnutzen.

1.11	Wie kann man in der Referenzimplementierung mit Identitäten testen?	Wenn der IDP einer Kasse eine Referenz-App bereitstellt, dann sollte diese auch Identitäten zum Testen bereitstellen. Funktionell macht es jedoch keinen Unterschied, ob man gegen die Referenz- oder die Testumgebung testet. Wenn jemand bereits über Testidentitäten verfügt oder Test-Aktenkonten mit entsprechender ID (KVNR) von seinem Enabler zur Verfügung gestellt bekommt, können wir diese auch in unseren IDP übernehmen. Dazu einfach eine Mail schreiben.
1.12	Wann kommt die GSIA-App?	Die GSIA-App wurde bereits auf GitHub veröffentlicht, sodass sie zumindest in Android Studio genutzt werden kann. Die Android-Version kann unter https://install.appcenter.ms/orgs/gematik/apps/gsia-android/distribution_groups/public/releases/16 bezogen werden. Es muss in den Einstellungen eingestellt werden, dass die GSIA für die Verwendung in der TU-Föderation gsi.dev.gematik.solutions Links und für die Verwendung in der RU-Föderation gsi-ref.dev.gematik.solutions Links öffnen darf. iOS kommt demnächst.
1.13	Wenn wir jedoch einen PAR an den IBM IDP schicken, dann kriegen wir diese Antwort: *at TLSSocket.emit (node:domain:489:12)" error=" Error: C01EF4DD01000000:error:0A000416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown:../deps/openssl/openssl/ssl/record /rec_layer_s3.c:1586:SSL alert number 46* Was bedeutet das?	Der Contenttype des Entity Statement ist falsch. - Aktueller Wert: application/octet-stream;charset=utf-8 - Erwarteter Wert: application/entity-statement+jwt
1.14	Es gibt eine Authentifikator-App von gematik, kann diese durch einen webbasierten Ablauf für Tests ersetzt werden? Idealerweise möchten wir die Authentifikator-App durch einige API-Aufrufe ersetzen, wenn wir mit der gematik Testumgebung arbeiten.	Die Authenticator-App sendet einfach nur ein GET an /auth mit dem Parameter "user_id = 12345678". Diesen Request können Sie einfach anders senden, dann sollte alles auch ohne die App funktionieren. **Zum Beispiel:** curl -v -H "X-Authorization:..." -X GET "https://gsi.dev.gematik.solutions/auth?user_id = 12345678"
1.15	Können wir die redirect_uris und iss noch nachträglich ändern?	Ja, es ist möglich, die `redirect_uris` und `iss` nachträglich zu ändern. Der Prozess dafür erfolgt über das E-Mail-Postfach, das bei der Registrierung verwendet wurde. Sie können die gewünschten Änderungen dort vornehmen.
1.16	Müssen DiGAs, die die gleiche Implementierung verwenden, einzeln für die TU registriert werden, oder ist hier eine einzige Registrierung ausreichend?	Bei DiGAs mit identischen Implementierungen ist für die Testung in der Testumgebung keine separate Registrierung erforderlich, sofern die Anbietererklärungen im Rahmen des Bestätigungsverfahrens abgegeben werden können. Allerdings, wenn es Unterschiede in den Daten, spezifisch im Entity Statement, gibt, ist eine erneute Registrierung notwendig. Bitte beachten Sie, dass für die Produktionsumgebung später für jede einzelne DiGA jeweils eine gesonderte Bestätigung und Registrierung zu beantragen ist.
1.17	Können wir mit einer Registrierung uns für die TU und RU gleichzeitig anmelden und wäre die Anmeldung an beiden Umgebungen überhaupt nötig/sinnvoll?	Sie können die Registrierung für die RU und TU gleichzeitig anstoßen. Eine Registrierung für die TU ist auf jeden Fall sinnvoll, weil unser gematik IDP nur in dieser Umgebung verwendet werden kann. Es kann sein, dass eine Registrierung in der RU für Integrationstests gegen die anderen sektoralen IDPs sinnvoll ist, aber vielleicht kommen Sie auch ohne diese Registrierung aus. Im Zweifel starten Sie einfach mit einer TU Registrierung und gucken wie weit Sie damit kommen.

1.18	Ist es erlaubt, die Daten meines Entity-Statements jederzeit zu ändern?	Änderungen am Entity-Statement sind nicht ohne Weiteres möglich. Der Federation Master prüft die Inhalte des Entity Statements gegen die bei der Registrierung angegebenen Werte. Konkret sind das: • Scopes • alles rund um den Schlüssel zur Signatur des Entity Statements • Organisationsname Jede Modifikation an diesen Werten muss der gematik offiziell mitgeteilt werden (läuft auch über die idp-registrierung; siehe Link). Ohne Mitteilung an die gematik geänder werden können z.B.: • redirect_uris • TLS-Clientzertifikat und ENC-Key im JWKS
1.19	Gibt es eine standardisierte Vorgehensweise, wie Informationen, z. B. das Fehlen einer E-Mail-Adresse von Krankenkassen, an uns kommuniziert werden?	Verhalten der IDPs ist wie folgt: A_22990-01
1.20	Können wir den Daten der IDPs vertrauen?	Bei der Nutzung von Daten, die von IDPs bereitgestellt werden, gibt es durch gematik spezifizierte Scopes und Claims, die als vertrauenswürdig gelten (z.B. KVNR). Es ist jedoch wichtig zu beachten, dass nicht alle Informationen gleichermaßen verlässlich sind. Insbesondere die E-Mail-Adresse kann ein weniger zuverlässiger Datenpunkt sein. Der Grund dafür ist, dass sie nicht zwingend vorhanden sein muss, und selbst wenn sie angegeben ist, kann sie veraltet sein. Daher sollte man beim Umgang mit solchen Informationen Vorsicht walten lassen und insbesondere die Email selbst überprüfen.

2. Fragen zur Kartenherausgabe / TI-Gateaway

2.1	Wie kann ein in Österreich ansässiges Unternehmen den Prozess zur Beantragung einer SMC-B und zur Anmeldung einer DiGA durchlaufen?	Hier eine kurze Übersicht der Schritte: **Identifikationsverfahren:** Laut D-TRUST ist das deutsche Postident-Verfahren auch für Inhaber eines österreichischen Passes in deutschen Postfilialen möglich. Alternativ bietet sich das BotschaftsIdent-Verfahren an, das durch deutsche Botschaften und Konsulate durchgeführt wird. Nähere Informationen zum Ablauf erhalten Sie bei der deutschen Botschaften/Konsulaten. **Versand:** Der Versand von Karten und PIN-Briefen per Kurier ist auch nach Österreich ohne zusätzliche Kosten möglich. **Antragsfelder:** Bei der Angabe von Wohnanschrift und Meldeadresse im Antrag kann Österreich ausgewählt werden, was für die Identifizierung erforderlich ist. Die Voreinstellung "Deutschland" bei der Organisationsadresse im Antrag ist festgelegt und kann nicht geändert werden, aber dieser Umstand ist im Antragsprozess sowohl für uns als auch für D-TRUST handhabbar. **Rechnungsstellung:** Die Rechnung kann Ihnen per E-Mail zugeschickt werden, bitte wählen Sie diese Option entsprechend aus. Vergewissern Sie sich, dass im Antragsformular auf der Seite der Organisationsdaten die Umsatzsteuer-Identifikationsnummer (UstID) eingetragen wird. Zögern Sie nicht, uns bei weiteren Fragen bzgl. Kartenherausgaben unter kartenherausgabe@gematik.de zu kontaktieren (insb. Hersteller aus anderen Ländern).
2.2	Muss ein DiGA-Hersteller, der mehrere digitale Gesundheitsanwendungen (DiGAs) anbietet, für jede einzelne DiGA eine separate SMC-B Karte beantragen?	Ja, es muss für jede einzelne DiGA im Verzeichnis eine separate SMC-B bestellt werden. Dies hat im Wesentlichen zwei Gründe: 1. Der Nutzer muss die ePA-Schreib- (und perspektivisch auch Lese-)berechtigung jeder DiGA einzeln vergeben können. 2. Bei Bedarf (z.B. in dem Fall, dass eine einzelne DiGA des Herstellers aus dem Verzeichnis gestrichen wird) muss jede SMC-B einer DiGA separat gesperrt werden können.

2.3	Wie verhält es sich mit der SMC-B Karte für DiGAs, die sich aktuell noch in der Entwicklung oder im Antragsverfahren befinden? Ab wann im Antragsprozess kann man eine SMC-B bestellen?	Gemäß der aktuellen Abstimmung mit dem BfArM kann die Beantragung einer SMC-B Karte für die Produktivumgebung erst nach der offiziellen Aufnahme der DiGA in das DiGA-Verzeichnis erfolgen. Für Testzwecke bietet die gematik jedoch spezielle Testkarten an, die über das Fachportal der gematik oder Ihren Enabler (RU-as-a-Service Anbieter) bestellt werden können - auch vor Listung als DiGA im verzeichnis. Weitere Informationen zu Testkarten und den Bestellprozess finden Sie auf der entsprechenden Seite des Fachportals der gematik.
2.4	Ist es möglich, die SMC-B Karte auch in der Referenzumgebung für Testzwecke einzusetzen?	Nein, die SMC-B Karte ist ausschließlich für den Einsatz im produktiven Betrieb vorgesehen und kann nicht in der Referenzumgebung für Testzwecke verwendet werden. Für Testzwecke bietet die gematik jedoch spezielle Testkarten an, die über das Fachportal der gematik oder Ihren Enabler (RU-as-a-Service Anbieter) bestellt werden können. Weitere Informationen zu Testkarten und den Bestellprozess finden Sie auf der entsprechenden Seite des Fachportals der gematik.
2.5	Ist für den Betrieb einer DiGA ein physisches Kartenterminal zur Nutzung der SMC-B erforderlich?	Ja, für den regulären Betrieb ist ein Kartenterminal notwendig, um die SMC-B Karte zu nutzen. Alternativ können DiGA-Hersteller auch auf die Dienste eines spezialisierten Dienstleisters, eines sogenannten Enablers, zurückgreifen, der einen TIaaS (Telematikinfrastruktur-as-a-Service) anbietet und die Einbindung des Kartenterminals in Ihre Infrastruktur mit Ihnen individuell bespricht.
2.6	Was geschieht mit bereits eingereichten Anträgen für eine SMC-B-Karte (Vor November)? Ist es erforderlich, den Antrag erneut zu stellen?	Nein, es ist nicht notwendig, bereits eingereichte Anträge für eine SMC-B-Karte neu zu stellen. Sollten im ursprünglichen Antrag Informationen, wie beispielsweise der Name der DiGA, gefehlt haben, werden die Antragstellenden von uns kontaktiert, um die erforderlichen Daten zu ergänzen.
2.7	Kann den Antrag jeder Angestellte stellen oder ist dies ausschließlich der Geschäftsführung vorbehalten?	Antragsteller müssen immer die Personen sein, die beim BfArM für die jeweilige DiGA als "Kontaktperson" gepflegt sind. Passen Sie bitte bei Bedarf vor Antragstellung die Daten im DiGA-Verzeichnis des BfArM entsprechend an. Änderungen der Adressen (auch der Ansprechpartner) im Antragsportal müssen dem BfArM mitgeteilt werden, damit diese dann durch das BfArM freigegeben werden können. Erst danach sind diese geänderten Daten über die Schnittstelle abrufbar, die die gematik zur Berechtigungsprüfung nutzt.
2.8	Welche Lieferzeit ergibt sich bei einem SMC-B Status "wird geprüft"?	Die Lieferzeit beträgt in der Regel 1,5 bis 2,5 Wochen durch D-Trust. Hinzu kommt die vorherige Bearbeitungszeit für die Identitätsprüfung (Ident).
2.9	Wie funktioniert das Botschafts-Ident?	"Botschaftsident" = entspricht Beglaubigung der Unterschrift des Antragstellers auf einem speziellen Dokument durch Bestätigung der Botschaft; das Vorgehen ist wie folgt: • die D-TRUST stellt das entsprechende Basisdokument zur Verfügung • der Antragsteller muss das Dokument befüllen; dabei ist die mit Antragsnummer des Kartenantrages anzugeben • ein Zeichnungsberechtigter der Botschaft beglaubigt der Unterschrift des Antragstellers durch Bestätigung mittels Stempel+Unterschrift • der Antragsteller übersendet das Dokument an die D-TRUST
2.10	Ich habe den Anmeldeprozess trotzdem versucht mit PostIdent und scheitere an der Eingabe der Postleitzahl - die ist in Österreich nur 4-stellig - das System lässt mich damit nicht weiter.	Bei der Eingabe der Meldeadresse können Sie als Land "Österreich" auswählen. Dann werden auch vierstellige Postleitzahlen akzeptiert. Bei weiteren Fragen, beispielsweise zur Lieferung, können Sie sich gerne an uns wenden.

3. Fragen zur GesundheitsID / IDPs:

3.1	Welche Kriterien müssen mTLS Client-Zertifikate erfüllen, einschließlich Gültigkeitsdauer und Subject-Angaben, **und ist der Einsatz einer Zertifikatskette möglich?**	Die beim TLS-Handshake verwendeten Zertifikate müssen durch den sektoralen IDP validiert werden können. Konkret bedeutet das, Authorization-Server müssen sicherstellen, dass die für die TLS Client Authentisierung gegenüber sektoralen IDPs verwendeten Schlüssel über das Entity Statement validiert werden können, indem für diese Zertifikate im Schlüsselsatz (jwks) des Fachdienstes abgelegt werden ("use = sig", x5c Objekt gesetzt). Nach [RFC8705-section 2.2 (https://www.rfc-editor.org/rfc/rfc8705.html#name-self-signed-certificate-mut)] ist der Authorization-Server erfolgreich authentifiziert, wenn das Zertifikat, das er während des Handshakes vorgelegt hat, mit einem der für diesen bestimmten Client registrierten Zertifikate übereinstimmt. Die TLS Authentisierungsschlüssel sind maximal 398 Tage gültig.
3.2	Wie ist das Vorgehen für einen Schlüsseltausch (use=sig)?	Die Signaturschlüssel, mit denen das Entity Statement des Fachdienstes signiert wird, müssen beim Federation Master (Vertrauensanker) über einen organisatorischen Prozess bekanntgegeben werden. Mehrere parallel existierende Schlüssel sind möglich. Details zum organisatorischen Prozess werden noch ergänzt.

3.3	Wie ist der Zusammenhang von *JWKS URL* und *JWKS* im Entity Statement?	Die Signaturschlüssel für das Entity Statement müssen im *jwks*-Claim des Entity Statements bekannt gegeben werden. Die Entschlüsselungsschlüssel (use=enc) und die mTLS Authentisierungsschlüssel (use=sig) befinden sich in den Metadaten der Relaying Party, entweder direkt unter dem *jwks*-Claim oder als Set unter einer URL (*jwks-Url*).
3.4	Kann die Gültigkeit des Entity Statement (claim *exp*) im Testsystem auf z.B. auf 30 Minuten gesetzt werden?	Prinzipiell kann im Testsystem nach Belieben konfiguriert werden. Allerdings muss die Interoperabilität berücksichtigt werden. Der sektorale IDP erneuert das Entity Statement zu einem Fachdienst derzeit alle zwei Stunden. Wenn Sie bei Ihren Integrationstests Probleme feststellen, dann sollten Sie auf jeden Fall diese abweichende Konfiguration im Hinterkopf behalten.
3.5	Ist die Regelung eines automatischen Logouts nach 10 Minuten Inaktivität auch dann anzuwenden, wenn das Authentifizierungstoken von unserem internen Identity Provider für die DiGA stammt? Gibt es eine Instanz, die die Einhaltung dieser Vorgabe prüft, und besteht das Risiko rechtlicher Konsequenzen durch Mitbewerber, falls wir uns nicht strikt an die Spezifikation halten?	Es besteht keine rechtliche Verpflichtung zur Implementierung eines automatischen Logouts nach 10 Minuten Inaktivität, wenn das Token von Ihrem internen IdP stammt; dies ist lediglich eine Empfehlung. Die Spezifikationen zum Logout-Intervall gelten primär für die Integration der GesundheitsID. Für DiGAs sind hauptsächlich die Datenschutzkriterien des BfArM ausschlaggebend. Bitte stellen Sie sicher, dass Ihre Datenschutzpraktiken diesen Kriterien entsprechen, um die Konformität mit den geltenden Vorschriften zu gewährleisten.
3.6	Muss ein Nutzer, der sich für die Registrierung in der App mit dem eID-Login über die Krankenkassen-App entschieden hat, bei jedem App-Start eine erneute Authentifizierung über die eID vornehmen, oder gibt es alternative Methoden für die Wiederanmeldung?	Nein, nach der Erstregistrierung über das eID-Login muss der Nutzer nicht bei jedem Start der App erneut das eID-Verfahren durchführen. Es stehen auch andere zulässige Authentifizierungsmethoden zur Verfügung. Die GesundheitsID kann dabei als eines der möglichen Verfahren für eine solche wiederkehrende Authentifizierung genutzt werden.
3.7	Ist die Nutzung der GesundheitsID nur zur Erlangung der KVNR erforderlich, oder sind DiGA-Hersteller gesetzlich dazu verpflichtet, diese generell zu unterstützen?	DiGA-Hersteller sind gesetzlich dazu verpflichtet, die GesundheitsID ab dem 1. Januar 2024 zu unterstützen. Der Nutzer muss die Möglichkeit bekommen, sich über die GesundheitsID an der DiGA anzumelden. Es ist nicht verboten, weitere Authentisierungsverfahren anzubieten, solange Sie den Anforderungen des BfArMs genügen. Für das Einstellen der Daten in die ePA des Nutzers ist die GesundheitsID allerdings zwingende Voraussetzung, da die KVNR nur so sicher bezogen werden kann.
3.8	Muss jede DiGA einzeln registriert werden oder muss die Registrierung separat für Android und iOS erfolgen?	Jede DiGA ist im Sinne der TI-Föderation eine Fachanwendung (Relying Party) und muss in der Föderation als eigener Fachdienst mit eigener client_id (iss), Schlüssel und scopes registriert werden. Die Registrierung bezieht sich auf den Authorization-Server des Fachdienstes. Die Clients des Fachdiensten - also Android-App, iOS-App oder Web-App - sind selbst nicht Teil der TI-Föderation und müssen auch nicht registriert werden.
3.9	Wie lange können vom Authorization-Server bereitgestellte Zugriffstoken gültig sein?	Es existiert keine feste Vorgabe bezüglich der Gültigkeitsdauer von Zugriffstoken für DiGAs. Empfohlen wird, dass die vom Authorization-Server ausgestellten Zugriffstoken eine maximale Gültigkeitsdauer von 10 Minuten haben sollten.
3.10	Können Authorization-Server Refresh-Token verwenden?	Authorization-Server können einen OAuth 2.0 Token Endpunkt anbieten um dort das Abrufen von Refresh-Token entsprechend https://datatracker.ietf.org/doc/html/rfc6749#section-1.5 zu ermöglichen.
3.11	Verifikation der Certificate Transparency fur TLS Verbindungen in die VAU - Ist alternativ auch eine CT Prüfung möglich?	Ja, eine CT Prüfung ist möglich. Diese Funktionalität wird durch aktuelle Standard Bibliotheken für TLS Verbindungen unterstützt kann dahingehend umgesetzt werden, dass im Pool der Vertrauenswürdigen CAs nur solche aufgenommen werden, welche dem CAB-Forum zugehören.
3.12	Kann ein Nutzer scopes, welche eine DiGA bei einem sektoralen IDP zu ihm anfragt, abwählen.	Der Nutzer kann seine Zustimmung zur Weitergabe der Daten einzelner scopes verweigern. Konkret lautet die Anforderung in der gemSpec_IDP_Sek dazu: *"A_22939 - Widerspruch zur Weitergabe einzelner Scopes* *Authenticator-Module des sektoralen IDP MÜSSEN dem Nutzer die Möglichkeit geben, einem Dienst einzelne scopes nicht zu übermitteln. Auch auf das Risiko hin, dass dieser Dienst dann nicht verwendet werden kann"*
3.13	Wo finden wir eine Liste aller Root Zertifikate aller Mitglieder des CAB Forum, damit wir diese importieren können?	Eine Liste der Root Zertifikate entnimmt man am besten aus dem Vertrauensraum der Browser bzw. eines aktuellen Betriebssystems.
3.14	Wie kann ich die Integration meiner DiGA in die Föderation beim BfArM nachweisen? Ist dazu eine Listung erforderlich?	In der Entwicklungsphase einer DiGA ist es möglich, in der Testumgebung zu arbeiten, auch ohne dass bereits eine Listung als DiGA vorliegt. Bitte sehen Sie sich für den weiteren Prozess nach dem erfolgreichen Testen den Leitfaden unter "Anmeldung an der DiGA mit der GesundheitsID" - "Umsetzung des Anwendungsfalls" an.

3.15	Wie soll man das Entity-Statement vom sektoral IDP mit dem Gegensatz vom Fed-Master vergleichen /validieren?	Jeder Schlüssel, der zum Signieren vom Entity Statement verwendet wird, ist im Federation Master hinterlegt. Wenn man vom gematik sektoralen IDP das Entity Statement abruft, kann man sehen, ob es signiert ist und kann den Federation Master nach dem Signatur Schlüssel des gematik sektoralen IDP fragen und damit die Signatur des Entity Statement validieren. Dann ist es vertrauenswürdig und die Informationen, die im Entity Statement stehen, können verwendet werden. In der Tabelle "*Body HTTP-Response an den Authorization-Server des Fachdienstes vom Federation Master zum Entity Statement des sektoralen IDP*" der gemSpec_IDP_Sek findet man unter *jwks* die Schlüssel welche der Federation Master für den sektoralen IDP (bzw. auch einen Fachdienst) kennt. Über die kid (Key-ID) kann hier ein Mapping zum verwendeten Schlüssel des Entity-Statement des sektoralen IDP erfolgen. Ein Beispiel-Request für die Teilnehmerauskunft beim Federation Master zum Teilnehmer gematik sektoraler IDP ist dokumentiert in IDP Wissensdatenbank/TI-Föderation/Umgebungen, Referenzimplementierungen, Codebeispiele/Federation Master - Umgebungen und Beispiele.
3.16	Gibt es UI-Vorgaben der gematik?	Es gibt keine spezifischen UI-Vorgaben der gematik. Allerdings bieten wir bestimmte Flows an, wie beispielsweise das Ausführen der Kassen-App durch die DiGA-App, die als Orientierung dienen können.
3.17	Müssen wir, wenn wir später in der Produktivumgebung live sind, einen IDP schreiben /implementieren?	Nein, es muss lediglich ein Authorization Server (RP) bereitgestellt werden, der mit einem zugelassenen IDP kommuniziert und sich von diesem Identitäten bestätigen lässt.
3.18	Können wir die GesundheitsID direkt mit einer Open-Source-Identitätsmanagement-Plattform unter Verwendung von OIDC/OAuth wie Keycloak oder Ory Kratos integrieren?	Die Vorgaben der gematik bewegen sich im Rahmen der Spezifikationen OpenID Connect, OAuth2 und OpenID Föderation und basieren soweit möglich auf den in dem Bereich definierten Standards. Allerdings werden Keycloak oder Ory Kratos voraussichtlich nicht out of the box die Funktionalitäten bereitstellen können um als Relying Party innerhalb der Föderation zu agieren. Wenn Sie KeyCloak oder Ory Kratos für die eigene OAuth2 Autorisierung Ihrer Anwendung nutzen möchten, sollten Sie die Security Best-Practices und Vorgaben der gematik für Fachdienste berücksichtigen.
3.19	Welche Claims können wir nach erfolgreicher Autorisierung erwarten? Zum Beispiel die E-Mail des Patienten oder andere Datenpunkte?	Die Claims/Scopes, die von den IDPs abgerufen werden können sind in gemSpec_IDP_Sek Tabelle 5 bzw. in der IDP-Wissensdatenbank zu finden. Grundsätzlich dürfen keine Scopes registriert und abgerufen werden, die über die Liste der verarbeiteten Daten hinausgeht, die dem BfArM im Rahmen des Antragsprozesses eingereicht und vom BfArM geprüft wird. Für die Testumgebung ist dies noch nicht relevant, da hier mit Testidentitäten gearbeitet wird.
3.20	Existiert eine offizielle Übersetzung für die GesundheitsID?	Eine offizielle Übersetzung für gibt es derzeit nicht. Jedoch könnte "HealthID" als angemessene Übersetzung dienen.
3.21	Wann wird das Logo für die GesundheitsID veröffentlicht und welche Verwendungszwecke hat es?	Das Logo für die GesundheitsID ist bereits über den folgenden Link verfügbar. Es ist für den Einsatz im Front-End Ihrer Digitalen Gesundheitsanwendungen vorgesehen, um eine einheitliche Identifikation und Bezugnahme auf die GesundheitsID zu ermöglichen.
3.22	Ist im Rahmen des Bestätigungsverfahrens ein Smoke-Test vorgesehen?	Nein, im Rahmen des Bestätigungsverfahrens ist kein Smoke-Test vorgesehen. Es besteht aber jederzeit die Möglichkeit eines bilateralen Austauschs mit der gematik. Anfragen hierzu bitte über diga@gematik.de
3.23	Wie können wir die Anzahl der Registrierungen für die GesundheitsID einsehen?	Informationen zur Anzahl der Registrierungen für die GesundheitsID können Sie über das TI Dashboard abrufen.

4. Fragen zur ePA (Anbindung, Schreiben, ...)

4.1	Ist der Login eines Versicherten über die GesundheitsID eine zwingende Voraussetzung dafür, dass DiGA-Betreiber Informationen in die ePA des Versicherten schreiben können, da nur so die Krankenversichertennummer (KVNR) zur Adressierung der ePA des Versicherten ermittelt werden kann?	Ja, derzeit ist der Login über die GesundheitsID eine zwingende Voraussetzung dafür, dass DiGA-Betreiber Daten in die ePA eines Versicherten schreiben können. Durch den Login mit der GesundheitsID wird die KVNR des Versicherten abgefragt, die unerlässlich ist, um auf die entsprechende ePA des Versicherten zuzugreifen und dort Daten eintragen zu können. Diese Vorgabe ist standardisiert und betrifft alle Anwendungen, die einen schreibenden Zugriff auf die ePA anstreben, nicht nur DiGAs.

4.2	Sind wir mit dem Besitz einer SMC-B Karte automatisch in den Anwendungen (z.B. ePA) gelistet?	Die Listung in den Anwendungen hängt nicht direkt vom Besitz der SMC-B Karte ab, sondern vom Eintrag in das Verzeichnisdienst der Telematikinfrastruktur. Die Listung erfolgt zum Zeitpunkt der Freischaltung der SMC-B Karte. Ab diesem Moment können Nutzer die DiGAs in den ePA-Apps sehen und für das Schreiben in der ePA berechtigen.

5. Fragen zu Anforderungen und den Spezifikationen

5.1	Wie muss/soll geprüft werden, ob eine DiGA die Anforderungen für die TI-Föderation zur Nutzung der GesundheitsID erfüllt?	DiGA Hersteller müssen erklären, dass sie die Anforderungen, welche im "Anwendungssteckbrief Digitale Gesundheitsanwendungen" gelistet sind, erfüllen. Diese Erklärung wird im Rahmen eines Bestätigungsverfahrens bei der gematik abgegeben. Das Verfahren kann ab Mitte Januar durchlaufen werden und erst dann wird der Anwendungssteckbrief (inkl. Verfahrensbeschreibung) veröffentlicht. Die DiGA-Hersteller sollten ihre Anwendung in der gematik Testumgebung auf Interoperabilität testen (siehe TI-Leitfaden für DiGA-Hersteller). Dem Hersteller eines Produkts wird empfohlen während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen.
5.2	Sind die Gebühren für das Bestätigungsverfahren pro DiGA zu entrichten?	Ja, die Gebühren für das Bestätigungsverfahren fallen pro DiGA an.
5.3	Verschiebt sich die Deadline für das Vorlegen der gematik Bestätigung, wenn nicht alle Authenticator Apps verfügbar sind?	Nein, die Verfügbarkeit von Authenticator Apps hat keinen Einfluss auf die Deadline für das Vorlegen der gematik Bestätigung. Es ist möglich, die Bestätigung zu beantragen, auch wenn nicht alle Authenticator Apps verfügbar sind. Die Hersteller müssen die Erklärungen im Rahmen des Bestätigungsverfahrens abgeben.