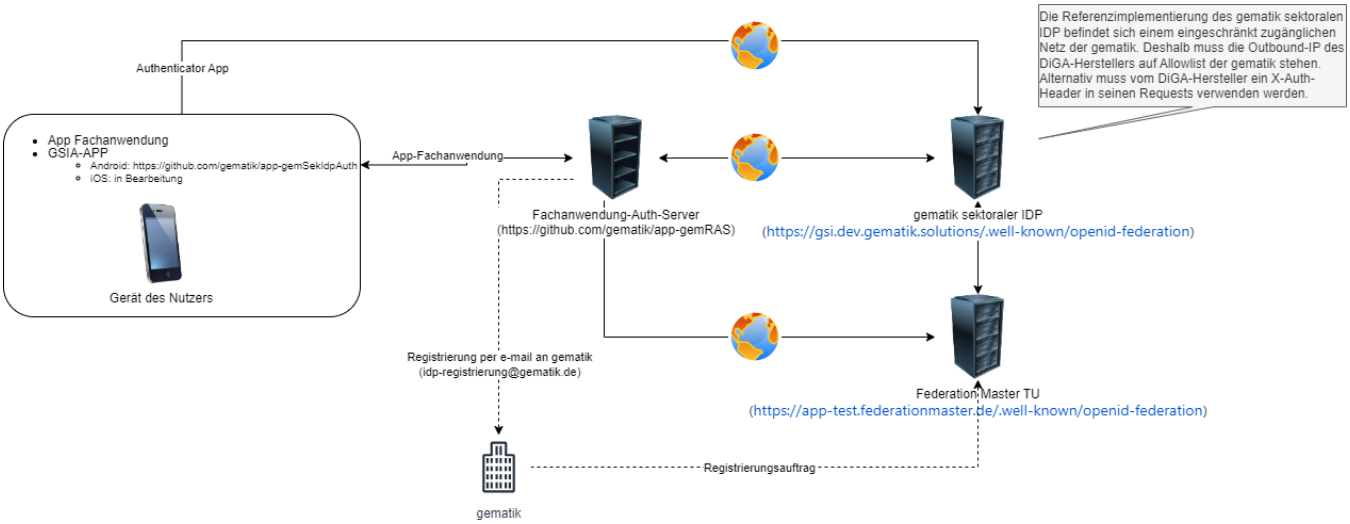
Fachdienste Test-Umgebungen

Verwendung des gematik sektoraler IDP und der GSIA-App zum Test von Fachanwendungen



Fachdienste der TI-Föderation können für Interoperabilitätstest ihrer Anwendung von der gematik bereitgestellte Referenzimplementierungen und Umgebungen nutzen. Die Referenzimplementierung besteht aus:

- gematik sektoreler IDP
  - stellt alle Schnittstellen eines sektoralen IDP entsprechend der Spezifikation zur Verfügung
  - ist beim Federation Master der Testumgebung registriert
  - enthält Testidentitäten
  - steht auch als Dockercontainer zum download zur Verfügung
- gematik Fachdienst
  - Referenzimplementierung eines Fachdienst Authorization Server
  - steht auch als Dockercontainer zum download zur Verfügung
  - https://github.com/gematik/app-gemRAS
- GSIA-App (Gematik Sektoraler IDP Authenticator)
  - zum gematik sektoralen IDP gehörende Authenticator-App
  - steht aktuell als Android-App zur Verfügung
  - bestätigt die Testidentitäten des sektoralen IDP
  - https://github.com/gematik/app-gemSekIdpAuth
- Federation Master
  - laufende Instanz in der Testumgebung
  - alle Teilnehmer der TI-Föderation in der Testumgebung sind hier registriert (neben der Referenzimplementierung gematik sektoraler IDP sind das auch zugelassene oder in Zulassung befindliche sektorale IDPs und Fachdienste)

In diesen Umgebungen können sie folgende Tests durchführen:

Entwicklungsbegleitende Integrationstest gegen den Federation Master

Voraussetzungen

- Keine, der Federation Master ist aus dem Internet erreichbar und seine Endpunkte können von jedem abgerufen werden

Testumfang

1. Entity Statement des Federation Masters über sich selbst abrufen Schritt 0 im App-App-Flow)
2. Liste aller in der TI-Föderation registrierter sektoraler IDPs abrufen (Schritt 0a im App-App-Flow)
    - Der Endpunkt zum Abruf der Liste aller in der TI-Föderation registrierter sektoraler IDPs kann aus dem Entity Statement (Test 1) entnommen werden
3. Liste aller Teilnehmer der TI-Föderation abrufen
    - Der Endpunkt zum Abruf der Liste aller in der TI-Föderation registrierter Teilnehmer kann aus dem Entity Statement (Test 1) entnommen werden
4. Entity Statement des Federation Masters über andere registrierte Teilnehmer der TI-Föderation abrufen (Schritt 1c App-App-Flow)
    - Der Endpunkt zum Abruf des Entity Statement über einen registrierter Teilnehmer kann aus dem Entity Statement (Test 1) entnommen werden
    - Aus der Liste der registrierte Teilnehmer (Test 3) kann dazu ein beliebiger Teilnehmer gewählt werden

Weiter Details siehe in den Beispiele für Tests gegen den Federation Master

Entwicklungsbegleitende Integrationstest gegen das Entity Statement des gematik sektoralen IDPs

Voraussetzungen

- Die Referenzimplementierung des gematik sektoralen IDP befindet sich einem eingeschränkt zugänglichen Netz der gematik. Deshalb muss die Outbound-IP des DiGA-Herstellers auf Allowlist der gematik stehen. Alternativ muss vom DiGA-Hersteller ein X-Auth-Header in seinen Requests verwenden werden. Dieser wird von der gematik auf Anfrage an diga@gematik.de kommuniziert.

Testumfang

1. Entity Statement des sektoralen IDP über sich selbst abrufen (Schritt 1a + 1b im App-App-Flow)
2. Teilnehmervalidierung des Teilnehmers gematik sektoraler IDP durch den Federation Master (Schritt 1c im App-App-Flow)

Weiter Details siehe in den Beispiele für Tests gegen den gematik sektoralen IDP

Entwicklungsbegleitende Integrationstest gegen den PAR-Endpunkt des gematik sektoralen IDPs

Voraussetzungen

- Die Referenzimplementierung des gematik sektoralen IDP befindet sich einem eingeschränkt zugänglichen Netz der gematik. Deshalb muss die Outbound-IP des DiGA-Herstellers auf Allowlist der gematik stehen. Alternativ muss vom DiGA-Hersteller ein X-Auth-Header in seinen Requests verwenden werden. Dieser wird von der gematik auf Anfrage an diga@gematik.de kommuniziert.
- Der DiGA-Hersteller muss den Registrierungsprozess für die Testumgebung durchlaufen haben. Der Registrierungsprozess schließt ein:
    - Vorlage eines korrektes Entity Statement für die Testumgebung (z.B. ist unter iss - also der Client-ID des Fachdienstes - die URL des Test-Authorization-Server des Fachdienstes anzugeben)
    - Vorlage des öffentlichen Schlüssel, mit dem das Entity Statement signiert wird
    - Angabe der benötigten scopes
    - Registrierung des Fachdienstes bei Federation Master der Testumgebung (wird durch die gematik durchgeführt)

Testumfang

1. Pushed Authorization Requests vom Auth-Server des Fachdienstes an den gematik sektoralen IDP (Schritt 2 im App-App-Flow)
2. Responses verarbeiten und Antwort auf Request vom Frontend mit HTTP-302 Redirect (Schritt 3+4 im App-App-Flow)
3. Deeplink auf dem Anwendergerät
    - ist die Authenticator-APP auf dem gleichen Gerät wie die Fachdienst-APP installiert, so wird diese geöffnet (Schritt 4+5 im App-App-Flow)
    - ist die Authenticator-APP nicht auf dem Gerät wie die Fachdienst-APP installiert, öffnet Browser mit Landing-Page des gematik sektoralen IDP (Schritt 4+5+6 im 2-Geräte-Flow

Entwicklungsbegleitende Integrationstest und um Authentisierung beim gematik sektoralen IDPs

Voraussetzungen

- Die Referenzimplementierung des gematik sektoralen IDP befindet sich einem eingeschränkt zugänglichen Netz der gematik. Deshalb muss die Outbound-IP des DiGA-Herstellers auf Allowlist der gematik stehen. Alternativ muss vom DiGA-Hersteller ein X-Auth-Header in seinen Requests verwenden werden. Dieser wird von der gematik auf Anfrage an diga@gematik.de kommuniziert.
- Der DiGA-Hersteller muss den Registrierungsprozess für die Testumgebung durchlaufen haben. Der Registrierungsprozess schließt ein:

    - Vorlage eines korrektes Entity Statement für die Testumgebung (z.B. ist unter iss - also der Client-ID des Fachdienstes - die URL des Test-Authorization-Server des Fachdienstes anzugeben)
    - Vorlage des öffentlichen Schlüssel, mit dem das Entity Statement signiert wird
    - Angabe der benötigten scopes
    - Registrierung des Fachdienstes bei Federation Master der Testumgebung (wird durch die gematik durchgeführt)
- Die GSIA-App ist installiert

Testumfang

1. Deeplink auf dem Anwendergerät
    - Die URI des Fachdienst Authorization-Server (redirect_url) muss als Deeplink auf dem Anwendergerät registriert sein
2. Durchreichen des vom gematik sektoralen IDP ausgestellten Authorization Code von der Fachdienst-App an dessen Authorization-Server (Schritt 8 im App-App-Flow)
3. Empfang des vom gematik sektoralen IDP ausgestellten Authorization Code (Schritt 9 im App-App-Flow)
4. Der Fachdienst Authorization-Server tauscht beim gematik sektoralen IDP den Authorization Code gegen das ID-Token (Schritt 10+11 im App-App-Flow)
5. Der Fachdienst Authorization-Server entschlüsselt erfolgreich das ID-Token

Hinweise

1. Ist die GSIA-App noch nicht verfügbar oder installiert, so können die Schritte 5-8 im App-App-Flow durch ein Mock ersetzt werden oder es wird die Authentisierung über unser Landing Page im Browser durchgeführt.
2. Es werden keine eigenen Testidentitäten benötigt und in den gematik sektoralen IDP eingebracht. Nach Bestätigung in der GSIA-App oder Authentisierung über unser Landing Page im Browser wird ein ID-Token zu bereits im gematik sektoralen IDP vorhanden Testidentitäten ausgegeben

Vollständiger Integrationstest gegen die Referenzimplementierung der gematik

Schritt	Beschreibung
Registrierung der Fachanwendung	E-Mail an idp-registrierung@gematik.de zur Registrierung am Federation Master TU ⚠ Details zur Registrierung werden dann nach Kontaktaufnahme durch die gematik mit dem Antragsteller besprochen
Laden der GSIA-App	Laden der GSIA-App auf Testgerät zur Nutzerauthentifizierung ⚠ • Die GSIA-App führt keine echte Nutzerauthentisierung durch, • Die Registrierung von Nutzern oder Geräten am sektoralen IDP der gematik ist nicht notwendig und auch nicht möglich. • Aktuell steht die GSIA-App nur als Code im GitHub bereit (https://github.com/gematik/app-gemSekIdpAuth)
Laden des Entity Statement Federation Master	download https://app-test.federationmaster.de/.well-known/openid-federation
Laden des Entity Statement des sektoralen IDP der gematik	sektoraler IDP der gematik: https://gsi.dev.gematik.solutions/.well-known/openid-federation ⚠ • Die Referenzimplementierung des gematik sektoralen IDP befindet sich einem eingeschränkt zugänglichen Netz der gematik. Deshalb muss die Outbound-IP des DiGA-Herstellers auf Allowlist der gematik stehen. Alternativ muss vom DiGA-Hersteller ein X-Auth-Header in seinen Requests verwenden werden. Dieser wird von der gematik auf Anfrage an diga@gematik.de kommuniziert.
Test der Anwendung	Test der Fachanwendung gegen die Schnittstellen des gematik sektoralen IDP der und des Federation Master Der Test der Nutzerauthentisierung ist erfolgreich, wenn der Fachanwendung ein ID-Token vom gematik sektoralen IDP zugestellt wurde. Als Nachweis des erfolgreichen Tests dient das entschlüsselte ID-Token.

Einschränkungen/Grenzen für entwicklungsbegleitende Integrationstest

Hier eine Übersicht über Funktionien, die (noch) nicht gegen den gematik sektorale IDP getestet werden können:

Funktion	Begründung
mTLS	Der gematik sektorale IDP validiert nicht das TLS-Clientzertifikat des Fachdienstes. Es wird nur einseitiges TLS gemacht. Da TLS außerhalb unser Anwendung terminiert, können wir an dieser Stelle keine Testmöglichkeit bieten.
Robustheit	Der gematik sektorale IDP beantwortet fehlerhafte Request mit entsprechenden Fehlerfällen. Es gibt aber keine Möglichkeit das Senden fehlerhafter Responses auszulösen. Daher eignet er sich nur begrenzt für die Durchführung von Negativ- oder Robustheitstests.
Performance	Der gematik sektorale IDP erfüllt nicht die Performancevorgaben eines produktiven sektoralen IDPs. Bitte verwenden Sie ihn daher nicht in eventuellen eigenen Lasttests. Es ist gut möglich, dass der davon abgeschossen werden würde.
Verfügbarkeit	Der gematik sektorale IDP kann immer mal wieder kurzzeitig nicht verfügbar sein. Z.B. in den Wartungsfenstern unserer IT oder wenn wir eine neue Version deployen (oder wenn uns jemand durch einen Lasttest abschießt). Falls wir länger unangekündigt offline sind, einfach per Mail nachfragen
ePA	Noch bietet unsere Testidentität keine Möglichkeit in eine ePA zu schreiben. Aber daran arbeiten wir

Akzeptanztests gegen zugelassenen sektoralen IDP

Kann ein von einem sektoralen IDP ausgestelltes ID-Token erfolgreich entschlüsselt werden, so wurde der Authentisierungsprozess in der Testumgebung auch erfolgreich durchlaufen.

Die finalen Tests sollten nicht gegen den gematik sektoralen IDP mit dessen GSIA-App sondern gegen einen von der gematik zugelassenen sektoralen IDP und dessen Authenticator-App in der Testumgebung ausgeführt werden. Weitere Informationen dazu folgen.

Umgebungen

Umgebung	Beschreibung	URL Entity Statement Federation Master	URL Entity Statement sektorale IDPs
Referenzumgebung (RU)	Die Referenzumgebung ist eine Integrationsumgebung. Hier kann das Zusammenspiel der beteiligten Komponenten und Systeme überprüft werden. dazu müssen die beteiligten Komponenten und Systeme einen möglichst produktionsnahmen Zustand besitzen. Im optimalen Fall ist die Überführung in die Produktionsumgebung ausschließlich durch Konfiguration möglich.	https://app-ref.federationmaster.de/.well-known/openid-federation	Information aus der Liste der registrierten sektoralen IDPs vom Federation Master
Testumgebung (TU)	Die Testumgebung dient der Überprüfung von Testkonzepten sowie von Schnittstellentest gegen beteiligte Komponenten. Die eigentliche Funktionalität hinter verwendeter Schnittstellen spielt eine untergeordnete Rolle. Um das Testziel zu erreichen können einzelne Komponenten durch Mock- oder Referenzimplementierungen ersetz werden.	https://app-test.federationmaster.de/.well-known/openid-federation	• Information aus der Liste der registrierten sektoralen IDPs vom Federation Master • u.a. gematik sektoraler IDP https://gsi.dev.gematik.solutions/.well-known/openid-federation
Produktionsumgebung (PU)	Die Produktionsumgebung ist für alle nutzenden Systeme und Nutzer zugänglich und muss - im Gegensatz zur Referenzumgebung - entsprechende Anforderungen an Hardware (z.B. RZ) und Sicherheit erfüllen. Für die Produktionsumgebung müssen die Produkte zugelassen werden. Je nach Produkt müssen dazu Zulassungskriterien erfüllt sein.	https://app.federationmaster.de/.well-known/openid-federation	Information aus der Liste der registrierten sektoralen IDPs vom Federation Master