

C_12598_Anlage_sekt_IDP

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

2 Änderung in gemSpec_IDP_Sek.....3

3 Änderungen in Steckbriefen.....18

3.1 Änderungen in gemProdT_IDP-Sek.....18

3.2 Änderungen in gemAnbT_IDP-Sek_KTR.....19

1 Änderungsbeschreibung

Die Spezifikationen gemSpec_IDP_Sek, gemSpec_IDP_FedMaster, gemSpec_IDP_FD setzen auf den Standard OpenID-Federation 1.0 - Draft 21 (https://openid.net/specs/openid-connect-federation-1_0-21.html) auf. Der Standard hat sich weiterentwickelt und ist seit 02/2026 final (https://openid.net/specs/openid-federation-1_0.html). Der OpenID Federation Standard wird dahin gehend weiter entwickelt, dass

- "OpenID Federation 1.1" alle Technologie unabhängigen Aspekte enthält (https://openid.net/specs/openid-federation-1_1.html)
- "OpenID Federation for OpenID Connect 1.1" aufsetzend auf "OpenID Federation 1.1" alle Aspekte für OIDC Architekturen enthält (https://openid.net/specs/openid-federation-connect-1_1.html)
- "OpenID Federation for Wallet Architectures 1.0" aufsetzend auf "OpenID Federation 1.1" alle Aspekte für Wallet Architekturen enthält (https://openid.net/specs/openid-federation-wallet-1_0.html)

Es ist zwingend notwendig, die Spezifikationen an den aktuellen Standard anzupassen, da sich wesentliche Bestandteile geändert haben.

Im Zuge dessen werden alle grundlegenden Informationen zur TI-Föderation in ein eigenes Dokument gemKPT_TI-Föderation ausgelagert, die eigentlichen Spezifikationen werden um die allgemeinen Informationen bereinigt. Damit wird gesichert, dass der allgemeine Blick nicht widersprüchlich in den den Spezifikation sondern zentral in einem Dokument gepflegt und weiterentwickelt werden.

Die Anlage enthält alle geplanten Anpassungen in gemSpec_IDP_Sek.

2 Änderung in gemSpec_IDP_Sek

Es wird Kapitel "2.1 Allgemeiner Überblick" wie folgt angepasst:

- Text und Abbildung werden entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

Aufbau und Funktionsweise der TI-Föderation ist in [gemKPT_TI] dargestellt und beschrieben.

Es wird Kapitel "2.2 Detaillierter Überblick" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

Es wird Kapitel "2.4.1 Schnittstellen" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

Es wird Kapitel "2.4.2 Akteure und Rollen" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

Es wird Kapitel "2.5 Nachbarsysteme und Interaktion" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

Es wird Kapitel "3.2 Vertrauenswürdige Ausführungsumgebung" wie folgt angepasst:

- Abbildung 4 "Schnittstellen der in der VAU laufenden Komponente des sektoralen IDP"

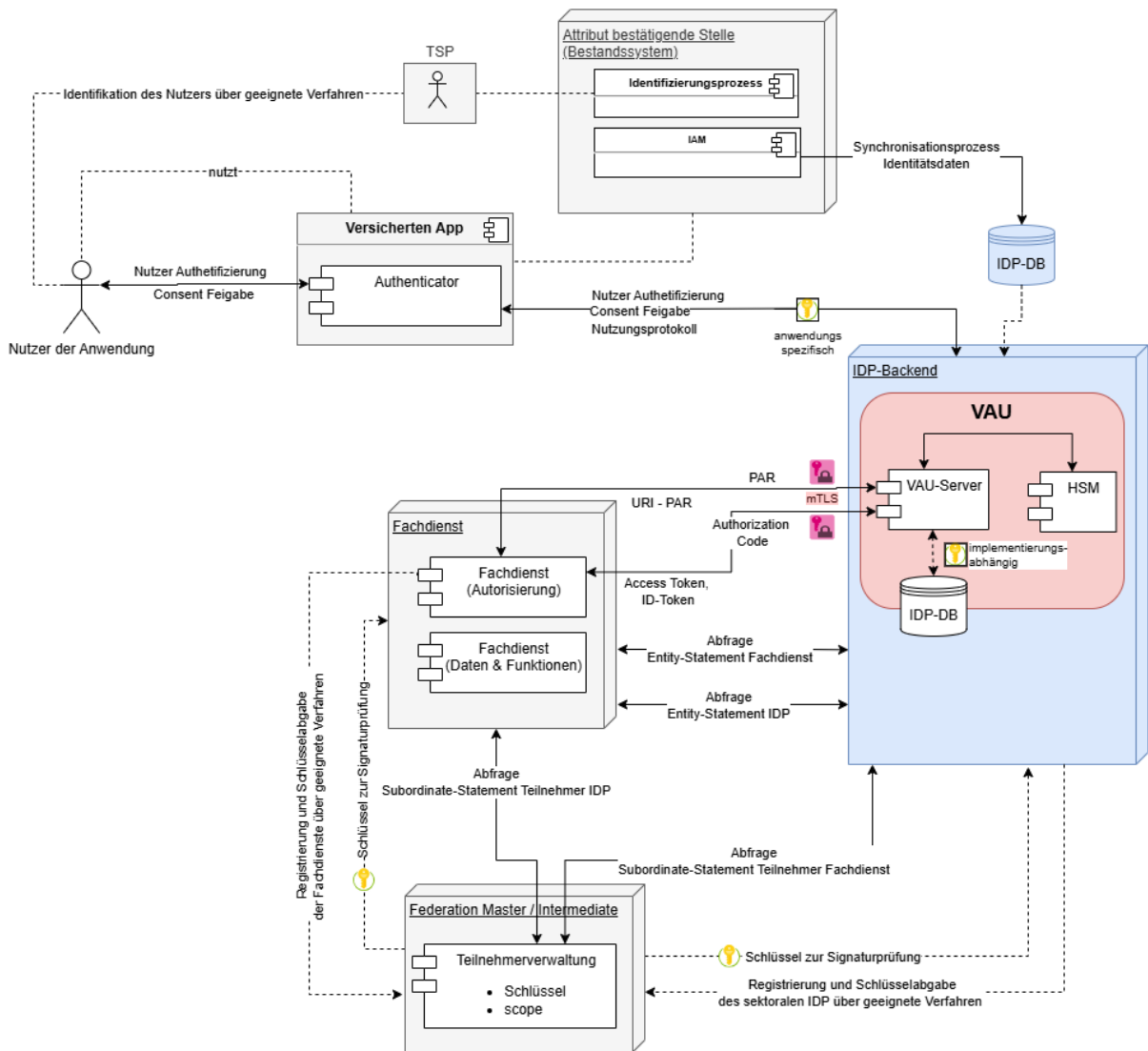


Abbildung 1 : Schnittstellen der in der VAU laufenden Komponente des sektoralen IDP

Tabelle 1: Vorgaben für die im sektoralen IDP befindlichen Endpunkte zur Ausführung in einer VAU

Schnittstelle	Gegenstelle	Beschreibung	VAU Ausführung
Pushed Authorization Request (PAR)	Fachdienst Authorization Server	Der Pushed Authorization Request enthält Informationen zum anfragenden Fachdienst und zum Scope der angeforderten Daten des Nutzers.	zwingend
Einlösen des	Fachdienst	Der Token-Request zum	zwingend

Authorization Code	Authorization Server	Einlösen des Authorization Code enthält Informationen zum Fachdienst. Der Response auf den Request enthält Informationen zum Nutzer.	
Abruf selbstsigniertes Entity Statement	Fachdienst Authorization Server	Der Fachdienst bezieht die Konfigurationsparameter , Adressen und Schlüssel des sektoralen IDP	optional
Abruf Subordinate Entity Statement zur Teilnehmerauskunft IDP	Federation Master	Der Schlüssel des Federation Master zum Verifizieren der von diesem signierten Subordiante Entity Statements wird sicher verwahrt.	optional
Abruf Subordinate Entity Statement zur Teilnehmerauskunft Fachdienst Authorization Server	Superior Entity (Federation Master, Intermediate)	Der Schlüssel der Superior Entity (Federation Master oder Intermediate) des Federation Master zum Verifizieren der von diesem signierten Entity Statements wird sicher verwahrt.	optional
Authentifizierung	Authenticator-Modul auf Endgerät des Nutzers	Die Ausprägung der Schnittstelle kann anwendungsspezifisch gestaltet werden.	optional
Consent-Freigabe und Initialer Authorization Request	Authenticator-Modul auf Endgerät des Nutzers	Es muss nachprüfbar gewährleistet sein, dass der Betreiber des sektoralen IDP keinen Zugriff auf die über die Schnittstelle transportierten Inhalte bezüglich des Anfragenden Dienstes erlangen kann.	zwingend
Aktualisierung der Identitätsdaten im sektoralen IDP	Anwendungssystem, welchen die Identitäten der Versicherten	Die Aktualisierung des Datenbestandes des sektoralen IDP erfolgt durch das	optional

	verwaltet (Attributbestätigende Stelle)	Bestandssystem der jeweiligen attributbestätigenden Stelle.	
Ablage und Abfrage der vom sektoralen IDP verwalteten schützenswerten Prozessdaten der Nutzerauthentifizierung	Datenbank für Prozessdaten der VAU	Die vom sektoralen IDP verwalteten schützenswerten Daten liegen verschlüsselt in einer Datenbank auf welche nur aus einer VAU zugegriffen werden kann. Die Datenbank kann innerhalb oder außerhalb der VAU betrieben werden. Bei einem Betrieb außerhalb der VAU muss gewährleistet sein, dass der Betreiber des sektoralen IDP keinen Zugriff auf die über die Schnittstelle transportierten Inhalte hat. <i>Hinweis: Schützenswerte Daten im Kontext der sektoralen IDP sind die Daten, welche innerhalb der VAU zum laufenden Authentifizierungsprozes s erzeugt bzw. gespeichert werden (client_id, state, redirect_uri, code_challenge, AUTHORIZATION_CODE, ID_TOKEN), sowie die Daten für das Nutzerprotokoll.</i>	optional

Es wird Kapitel "4.1 Entity Statement des sektoralen IDP" wie folgt angepasst:

Implementierung

Alt:

A_23413 -Entity Statement vom Federation Master abrufen

Der sektorale IDP MUSS zur Teilnehmerbestätigung anfragender Fachdienste deren Entity Statements vom Federation Master entsprechend [gemSpec_IDP_FedMaster#AF_10101] einholen.[<=, ,]

A_23132-01 -Regelmäßige Aktualisierung der Entity Statements bekannter Fachdienste

Der sektorale Identity Provider SOLL die Entity Statements für bekannte Fachdienste nach 12 Stunden erneut herunterladen.【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

A_23413, A_23132-01 entfällt durch die Zuordnung von A_28848 zum sekt. IDP

Neu:Zuweisung - A_28848

A_28848 -Validierung der Vertrauenskette eines TI-Föderation-Teilnehmers

Teilnehmer der TI-Föderation, welche mit anderen Teilnehmern der TI-Föderation kommunizieren wollen, MÜSSEN das Entity Statement des anderen TI-Föderation-Teilnehmers abrufen und gemäß der Regeln [[OpenID Federation 1.1](#)] ("Entity Statement Validation") validieren, sowie die Vertrauenskette gemäß [[OpenID Federation 1.1](#)] ("Resolving the Trust Chain and Metadata") prüfen. Der Abruf des Entity Statement sollte alle 12h und MUSS innerhalb von 24h erfolgen.

【<=, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, extNutz_GID, IDP-D, digi_ID_OGR, IDP-Sek, IDP_FedMaster, Sich.techn. Eignung: Anbietererklärung, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung】

Neu:Zuweisung - A_29019

A_29019 -Abruf eines Subordinate Statement abweichend von OpenID Federation 1.1 (befristet)

Der Abruf eines Subordinate Statement eines Teilnehmers zu einem anderen Teilnehmer bei dessen Superior Entity MUSS abweichend zu [[OpenID Federation 1.1](#)] ("Fetch Subordinate Statement Request") ein HTTP-GET Request mit folgenden Parametern an den federation_fetch_endpoint der Superior Entity sein:

Tabelle 2: Teilnehmer Validierung Abfrage - Request-Parameter

Attribut	Werte / Typ	Anmerkung
iss	string, URL nach [RFC1738]	Identifizier (iss) der Subordinate Entity (Federation Master oder Intermediate-Entity), bei welcher der Teilnehmer (sub) registriert ist.
sub	string, URL nach [RFC1738]	Identifizier (iss) des angefragten Teilnehmers aus dessen Entity Statement

Hinweis: Eine Umstellung auf den aktuellen Standard entsprechend [[OpenID Federation 1.1](#)] ("Fetch Subordinate Statement Request") kann erst erfolgen, wenn die API des Federation Master angepasst wurde.【<=, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, extNutz_GID, IDP-D, digi_ID_OGR, IDP-Sek, IDP_FedMaster, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung】

Alt:

A_23133 -Maximale Gültigkeitsdauer der Entity Statements bekannter Fachdienste

Der sektorale Identity Provider MUSS die Entity Statements für bekannte Fachdienste nach maximal 24 Stunden verwerfen.【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

A_23133 entfällt durch die Zuordnung von A_28857 zum sekt. IDPNeu:Zuweisung - A_28857**A_28857 -Maximale Gültigkeitsdauer und regelmäßige Erneuerung des Entity Statement eines TI-Föderation-Teilnehmers**

Teilnehmer der TI-Föderation MÜSSEN ihr Entity Statement bei Änderungen oder vor dem zeitlichen Ablauf neu ausstellen. Die maximale Gültigkeitsdauer - gegeben durch die Differenz der Attributwerte exp-iat - darf 24 Stunden nicht überschreiten. [≤, Aktensystem_ePA, Anw_DiGA, extNutz_GID, IDP-D, digi_ID_OGR, IDP-Sek, IDP_FedMaster, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

Hinweis: Ist ein Teilnehmer der TI-Föderation temporär nicht erreichbar, so sollte das Herunterladen der Entity Statements über den Teilnehmer weiter (z.B. stündlich) versucht werden.

Alt:**A_22662 -Registrierung beim Federation Master durch organisatorischen Prozess**

Der Anbieter des sektoralen IDP MUSS seine öffentlichen Schlüssel für die Signatur des selbst signierten Entity Statement über einen vom Federation Master angebotenen organisatorischen Prozess bei diesem bekannt machen. [≤, Anb_IDP-Sek_KTR, organ./betriebl. Eignung: Anbietererklärung]

A_22662 entfällt durch die Zuordnung von A_28879 zum sekt. IDPNeu:Zuweisung - A_28879**A_28879 -Registrierung von Teilnehmern in der TI-Föderation durch organisatorischen Prozess**

Ein Teilnehmer der TI-Föderation MUSS seinen öffentlichen Schlüssel für die Signatur des selbst-signierten Entity Statement (federation entity signing key) über einen organisatorischen Prozess bei der Superior Entity (Federation Master oder Intermediate) bekannt machen, bei welcher der Teilnehmer als Subordinate Entity registriert werden soll. Nach erfolgreicher Registrierung wird dem Teilnehmer der öffentliche Schlüssel übermittelt, mit dem das Entity Statement des Federation Master signiert ist (federation entity signing key). Der Teilnehmer MUSS diesen Schlüssel speichern und zur Validierung einer Vertrauensketten gemäß A_28848* verwenden. [≤, Anw_DiGA, extNutz_GID, Anb_IDP-D, Anb_IDP-Sek_KTR, digi_ID_OGR, Anb_Aktensystem_ePA, Anb_IDP_FedMaster, organ./betriebl. Eignung: Anbietererklärung]

Alt:**A_22643-01 -Entity Statement des sektoralen IDP**

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß [OpenID Federation 1.0#name-entity-statement] bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 3: Header des Entity Statement des sektoralen IDP

Name	Werte / Wertebereich
alg	string, zulässiger Wert "ES256"

kid	string Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string zulässiger Wert "entity-statement+jwt"

149 **Tabelle 4 :Allgemeine Attribute im well-known-Dokument des sektoralen IDP**

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]
sub	string, URL nach [RFC1738]
iat	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
exp	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
jwks	Set von JWK [RFC7517]
authority_hints	[string] zulässiger Wert: iss aus dem Entity Statement des Federation Master
metadata	string, zulässiger Wert: "openid_provider"

150 **Tabelle 5 :Attribute des Metadatenblocks openid_provider im well-known-Dokument des**
151 **sektoralen IDP**

Name	Werte
issuer	string, URL nach [RFC1738]
signed_jwks_uri(*)	string, URL nach [RFC1738]
jwks (*)	Set von JWK [RFC7517]
authorization_endpoint	string, URL nach [RFC1738]
token_endpoint	string, URL nach [RFC1738]

pushed_authorization_request_endpoint	string, URL nach RFC1738
client_registration_types_supported	[string] zulässiger Wert: "automatic"
subject_types_supported	[string] zulässiger Wert: "pairwise"
response_types_supported	[string] zulässiger Wert: "code"
scopes_supported	[string], Wertebereich: "openid", "<weitere Scopes nach A_22989*>"
claims_supported	[string], Wertebereich: "<Claims nach A_22989*>"
claims_parameter_supported	boolean, Wertebereich: true/false
response_modes_supported	[string] zulässiger Wert: "query"
grant_types_supported	[string] zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean, Wertebereich: true/false
token_endpoint_auth_methods_supported	[string] erforderlicher Wert: "self_signed_tls_client_auth"
id_token_signing_alg_values_supported	[string] erforderlicher Wert: "ES256"
id_token_encryption_alg_values_supported	[string] erforderlicher Wert: "ECDH-ES"
id_token_encryption_enc_values_supported	[string] erforderlicher Wert: "A256GCM"
user_type_supported	[string] zulässiger Wert: "IP" (Insured Person)
<i>ti_features_supported {</i>	

id_token_version_supported	[string] zulässige Werte in Liste: "1.0.0", "2.0.0"
----------------------------	---

Tabelle 6 :Attribute des Metadatenblocks federation_entity im well-known-Dokument des sektoralen IDP

(*) - gemäß [OpenID Federation 1.0] darf der Metadatenblock nur entweder signed_jwks_uri oder jwks enthalten.

Name	Werte / Wertebereich
organization_name	String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüß\w\ \-\.&\+*V]{1,128}\$

【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

Implementierung

Neu:

A_22643-02 -Entity Statement des sektoralen IDP

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß[OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 7: Header des Entity Statement des sektoralen IDP

Name	Werte / Wertebereich
alg	string, zulässiger Wert "ES256"
kid	string, UUID7-Format [RFC9562#name-uuid-version-7] Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string, zulässiger Wert "entity-statement+jwt"

Tabelle 8 :Allgemeine Attribute im well-known-Dokument des sektoralen IDP

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]
sub	string, URL nach [RFC1738]

iat	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
exp	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]
jwks	Set von JWK [RFC7517]
authority_hints	[string] zulässige Werte gemäß [OpenID Federation 1.1] ("Claims that MUST or MAY Appear in Entity Configurations but Not in Subordinate Statements") - authority_hints
metadata	JSON Object, erforderlicher Wert: "openid_provider"

Tabelle 9 : Attribute des Metadatenblocks openid_provider im well-known-Dokument des sektoralen IDP

Name	Werte
issuer	string, URL nach [RFC1738]
signed_jwks_uri(*)	string, URL nach [RFC1738]
jwks (*)	Set von JWK [RFC7517]
authorization_endpoint	string, URL nach [RFC1738]
token_endpoint	string, URL nach [RFC1738]
pushed_authorization_request_endpoint	string, URL nach [RFC1738]
organization_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - organization_name) Wertebereich: ^[a-üÄ-Üß\w\ \-\.\+*V]{1,128}\$
display_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - display_name) Wertebereich: ^[a-üÄ-Üß\w\ \-\.\+*V]{1,128}\$
keywords	[string] (gemäß [OpenID-Federation

	"Informational Metadata Extensions"] - keywords) erforderliche Werte: "product_type_version:<von der gematik zugelassene Produkttyp-Version>" "product_type:<von der gematik zugelassener Produkttyp>"
contacts	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions"] - contacts) erforderlicher Wert in Liste: "<E-Mail-Adresse für Supportanfragen>"
logo_uri	string, URL nach [RFC1738] zulässiger Wert: <URL>*.png
client_registration_types_supported	[string] zulässiger Wert: "automatic"
subject_types_supported	[string] zulässiger Wert: "pairwise"
response_types_supported	[string] zulässiger Wert: "code"
scopes_supported	[string], Wertebereich: "openid", "<weitere Scopes nach A_22989*>"
claims_supported	[string], Wertebereich: "<Claims nach A_22989*>"
claims_parameter_supported	boolean, Wertebereich: true/false
response_modes_supported	[string] zulässiger Wert: "query"
grant_types_supported	[string] zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean, Wertebereich: true/false zulässiger Wert: true
token_endpoint_auth_methods_supported	[string] erforderlicher Wert: "self_signed_tls_client_auth"

id_token_signing_alg_values_supported	[string] erforderlicher Wert: "ES256"
id_token_encryption_alg_values_supported	[string] erforderlicher Wert: "ECDH-ES"
id_token_encryption_enc_values_supported	[string] erforderlicher Wert: "A256GCM"
user_type_supported	[string] zulässiger Wert: "IP" (Insured Person)
ti_features_supported {	
id_token_version_supported	[string] zulässige Werte in Liste: "1.0.0", "2.0.0"

(*) - gemäß [\[OpenID-Federation 1.0\]](#) - "Usage of jwks, jwks_uri, and signed_jwks_uri in Entity Metadata" darf der Metadatenblock nur entweder signed_jwks_uri oder jwks enthalten. [\leq , IDP-Sek, funkt. Eignung: Test Produkt/FA]

Implementierung

Alt:

A_22710 -Vorlaufzeit bei geplantem Schlüsselwechsel

Der Anbieter des sektoralen IDP MUSS Signaturschlüssel im Rahmen eines geplanten Schlüsselwechsels mindestens 24 Stunden vor Verwendung in seinem jwks-Schlüsselsatz veröffentlichen und beim Federation Master über einen organisatorischen Prozess hinterlegen. [\leq , Anb_IDP-Sek_KTR, Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

Hinweis: Nicht betroffen von dieser Anforderung sind kurzfristig notwendige Schlüsselwechsel, z. B. aufgrund von Sicherheitsvorfällen. Diese Maßnahmen sind beispielsweise über security incidents abzuwickeln. Die Bearbeitung solcher kurzfristigen Schlüsselwechsel muss die Aktualisierung beim Federation Master mitberücksichtigen, da es ansonsten zu Verarbeitungsfehlern wegen ungültiger Schlüssel kommen kann.

A_22710 und Hinweis entfällt durch die Zuordnung von A_28859 zum sekt. IDP

Neu:Zuweisung A_28859

A_28859 -Vorlaufzeit bei geplantem Schlüsselwechsel Signaturschlüssel für Entity Statements

Im Rahmen eines geplanten Schlüsselwechsels der Signaturschlüssel MÜSSEN Teilnehmer der TI-Föderation den neuen öffentlichen Signaturschlüssel mindestens 24 Stunden vor der Verwendung im jwks-Schlüsselsatz im Entity Statement zusätzlich zum aktuell gültigen Signaturschlüssel veröffentlichen. Dieser Signaturschlüssel ist der neue Schlüssel, mit dem der Teilnehmer sein Entity Statement (federation entity signing key)frühestens 24 Stunden nach dieser Veröffentlichung signiert. Der Schlüsselwechsel sollte entsprechend [\[OpenID Federation 1.1\]](#) ("Updating Metadata, Key Rollover, and Revocation") erfolgen.

Hinweis: Nicht betroffen von dieser Anforderung sind kurzfristig notwendige Schlüsselwechsel, z. B. aufgrund von Sicherheitsvorfällen. Diese Maßnahmen sind

beispielsweise über Security Incidents abzuwickeln. Die Bearbeitung solcher kurzfristigen Schlüsselwechsel muss die Aktualisierung beim Federation Master bzw. Intermediate mit berücksichtigen, da es ansonsten zu Verarbeitungsfehlern wegen ungültiger Schlüssel kommen kann. [≤, Anw_DiGA, Anb_IDP-D, Anb_IDP-Sek_KTR, digi_ID_OGR, Anb_Aktensystem_ePA, Anb_IDP_FedMaster, organ./betriebl. Eignung: Anbietererklärung]

Alt:

A_27988 -Bekanntgabe von Änderungen im Entity Statement - Anbieter sek IDP KTR

Der Anbieter sektoraler IDP KTR MUSS geplante Änderungen der folgenden Claims im Entity Statement vor deren Veröffentlichung bei dem Federation Master über einen organisatorischen Prozess beantragen:

- Änderungen des Schlüsselsets, mit dem das Entity Statement signiert wird -jwks,
- Änderungen des in der TI-Föderation propagierten Organisationsnamens - *federation_entity.organization_name*.

[≤, Anb_IDP-Sek_KTR, organ./betriebl. Eignung: Betriebshandbuch]

A_27988 entfällt, jwks ist über Key Rollover nach Standard abgedeckt und openid_provider.organization_name muss nicht vorab angezeigt werden. Änderungen im Entity Statement werden von "Regine" geprüft

Es wird Kapitel "4.2.1 Anforderung an die Schnittstelle zum Authorization Server des Fachdienstes" wie folgt angepasst:

Alt:

A_22650 -automatische Registration von Fachdiensten

der sektorale IDP MUSS eine automatische Registrierung eines Fachdienstes bei Übermittlung eines Authorization Request mit *self_signed_tls_client_auth* gemäß [OpenID Federation 1.0] durchführen, sofern dieser Dienst nicht bereits am IDP registriert wurde. Nach Abruf des Entity Statement des Fachdienstes beim Fachdienst selbst MUSS der sektorale IDP beim Federation Master dessen Entity Statement zum Fachdienst gemäß [OpenID Federation 1.0] abrufen und so dessen Zugehörigkeit zur Föderation bestätigen zu lassen. Anschließend registriert der sektorale IDP den Fachdienst und importiert dessen Schlüssel für die Authentisierung und Verschlüsselung von Token. [≤, IDP-Sek, Sich.techn. Eignung: Produktgutachten]

Implementierung

Neu:

A_22650-01 -Automatische Registrierung von Fachdiensten

Der sektorale IDP MUSS eine automatische Registrierung eines Fachdienstes *Authorization Servers* bei Übermittlung eines Authorization Request mit *self_signed_tls_client_auth* gemäß [OpenID Federation 1.1] durchführen, sofern dieser Dienst nicht bereits am IDP registriert wurde. ~~Nach Abruf des Entity Statement des Fachdienstes beim Fachdienst selbst MUSS der sektorale IDP Federation Master dessen Entity Statement zum Fachdienst gemäß [OpenID Federation 1.0] abrufen und so dessen Zugehörigkeit zur Föderation bestätigen zu lassen.~~ Der sektorale IDP MUSS das Entity

Statement des Fachdienst Authorization Server abrufen und gemäß A_28848* validieren. Anschließend registriert der sektorale IDP den Fachdienst Authorization Server und importiert dessen Schlüssel für die Authentisierung und Verschlüsselung von Token. [≤, IDP-Sek, Sich.techn. Eignung: Produktgutachten]

Es wird Kapitel "4.2.4.2 Token-Endpunkt Ausgangsdaten" wie folgt angepasst:

Alt:

A_22655-02 -Signatur des "ID Token" des sektoralen IDP

Der sektorale IDP MUSS die ID Token unter Verwendung eines privaten Schlüssels, der zu einem direkt unter jwk im Entity Statement stehenden oder unter signed_jwks_uri referenzierten öffentlichen Schlüssel gehört, signieren [OpenID Connect Federation 1.0].

Zum öffentlichen Schlüssel des verwendeten Schlüsselpaares MUSS es ein Signaturzertifikat des Typs C.FD.SIG und der technischen Rolle „oid_idpd_sek“ gemäß [gemSpec_Krypt#Abschnitt 3.7] aus der Komponenten-PKI der TI geben, welches im Parameter x5c des ID Token Headers enthalten ist. [≤, IDP-Sek, funkt. Eignung: Test Produkt/FA]

redaktionell

Neu:

A_22655-03 -Signatur des "ID Token" des sektoralen IDP

Der sektorale IDP MUSS die ID Token unter Verwendung eines privaten Schlüssels, der zu einem direkt unter openid_provider.jwk im Entity Statement stehenden oder unter openid_provider.signed_jwks_uri referenzierten öffentlichen Schlüssel gehört, signieren [OpenID Federation 1.1].

Zum öffentlichen Schlüssel des verwendeten Schlüsselpaares MUSS es ein Signaturzertifikat des Typs C.FD.SIG und der technischen Rolle „oid_idpd_sek“ gemäß [gemSpec_Krypt#Abschnitt 3.7] aus der Komponenten-PKI der TI geben, welches im Parameter x5c des ID Token Headers enthalten ist. [≤, IDP-Sek, funkt. Eignung: Test Produkt/FA]

redaktionell

Hinweis unter A_22989-02

Hinweis: Die Regel zur Festlegung des Geburtsdatums bei unbekanntem Tag bzw. Monat basiert auf den [Datensätze und Datenbausteine sowie Fehlerkatalog] (https://www.informationsportal.de/wp-content/uploads/GemRS_Anlage_09.4_Vers-8.00.pdf) (https://www.gkv-datenaustausch.de/media/dokumente/arbeitgeber/deuev/rundschreiben_anlagen/04_Gem_RS_Anlage_9.4_Vers_8.00.pdf)

Es wird Kapitel "5.1 Funktionsmerkmale Authenticator-Modul" wie folgt angepasst:

- Abbildung 5 "Systemkontext Authenticator-Modul" - Federation Master --> Superior

295

296 [Es wird Kapitel "7 Anhang B - Abläufe" wie folgt angepasst:](#)

297 Texte und Abbildung werden entfernt, es wird auf gemKPT_TI-Föderation verwiesen.

298

299

300

301

302

303

304

305

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_IDP-Sek

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 10: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22643-01	Entity Statement des sektoralen IDP	gemSpec_IDP_Sek
A_22643-02	Entity Statement des sektoralen IDP	gemSpec_IDP_Sek
A_22655-02	Signatur des "ID Token" des sektoralen IDP	gemSpec_IDP_Sek
A_22655-03	Signatur des "ID Token" des sektoralen IDP	gemSpec_IDP_Sek
A_23132-01	Regelmäßige Aktualisierung der Entity Statements bekannter Fachdienste	gemSpec_IDP_Sek
A_23133	Maximale Gültigkeitsdauer der Entity Statements bekannter Fachdienste	gemSpec_IDP_Sek
A_23413	Entity Statement vom Federation Master abrufen	gemSpec_IDP_Sek

Tabelle 11: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22650	automatische Registrierung von Fachdiensten	gemSpec_IDP_Sek
A_22650-01	Automatische Registrierung von Fachdiensten	gemSpec_IDP_Sek
A_28848	Validierung der Vertrauensketten eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster

Tabelle 12: Anforderungen zur funktionale Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28857	Maximale Gültigkeitsdauer und Regelmäßige	gemSpec_IDP_FedMaster

	Erneuerung des Entity Statement eines TI-Föderation Teilnehmers	
--	---	--

3.2 Änderungen in gemAnbT_IDP-Sek_KTR

Tabelle 13: Anforderungen zur organisatorischen / betrieblichen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22710	Vorlaufzeit bei geplantem Schlüsselwechsel	gemSpec_IDP_Sek
A_28859	Vorlaufzeit bei geplantem Schlüsselwechsel Signaturschlüssel für Entity Statements	gemSpec_IDP_FedMaster
A_22662	Registrierung beim Federation Master durch organisatorischen Prozess	gemSpec_IDP_Sek
A_28879	Registrierung von Teilnehmer in der TI-Föderation durch organisatorischen Prozess	gemSpec_IDP_FedMaster

Tabelle 14: Anforderungen zur organisatorischen / betrieblichen Eignung "Betriebshandbuch"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_27988	Bekanntgabe von Änderungen im Entity Statement - Anbieter sek IDP KTR	gemSpec_IDP_Sek