
C_11742_Anlage

Änderung in gemSpec_IDP_FedMaster

3.3.1 Akzeptanzkriterien - Entity Statement bereitstellen

Das Akzeptanzkriterium "AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation" wird erweitert. ML-128452 wird deshalb durch ML-152179 ersetzt.

Durch die Zuordnung des neuen Akzeptanzkriterium das AF_10101 durch das AF_10101-01 ersetzt.

Alt:

ML-128452 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation

Der Payload des JWS-Tokens enthält diese Informationen bezüglich des angefragten Teilnehmers der Föderation (siehe auch [gemSpec_IDP_Sek - Anhang B - Abläufe](#)):

- iss = URL - Identifizier Federation Master
- sub = URL - Identifizier des angefragten Teilnehmers
- iat = long Wert - Ausstellungszeitpunkt des Abrufs (Alle time-Werte in Sekunden seit 1970)
- exp = long Wert - Ablaufzeitpunkt der Gültigkeit des Abrufs (Alle time-Werte in Sekunden seit 1970)
- jwks = JWKS Objekt - öffentlicher Schlüssel des angefragten Teilnehmers.
- aud = URL - Identifizier des anfragenden Teilnehmers. Wenn der aud-Parameter im Fetch Entity-Statement-Request des anfragenden Teilnehmers vorhanden ist, MUSS der aud Parameter in der Fetch Entity-Statement-Response vorhanden sein und genau diesen Wert annehmen

Neu:

ML-152179 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation

Der Payload des JWS-Tokens enthält diese Informationen bezüglich des angefragten Teilnehmers der Föderation (siehe auch [gemSpec_IDP_Sek - Anhang B - Abläufe](#)):

- iss = URL - Identifizier Federation Master
- sub = URL - Identifizier des angefragten Teilnehmers
- iat = long Wert - Ausstellungszeitpunkt des Abrufs (Alle time-Werte in Sekunden seit 1970)
- exp = long Wert - Ablaufzeitpunkt der Gültigkeit des Abrufs (Alle time-Werte in Sekunden seit 1970)
- jwks = JWKS Objekt - öffentlicher Schlüssel des angefragten Teilnehmers.
- aud = URL - Identifizier des anfragenden Teilnehmers. Wenn der aud-Parameter im Fetch Entity-Statement-Request des anfragenden Teilnehmers vorhanden ist,

40 MUSS der `aud` Parameter in der Fetch Entity-Statement-Response vorhanden sein
41 und genau diesen Wert annehmen

42 Für registrierte Relying Parties (Fachdienste) MÜSSEN zusätzlich diese Informationen im
43 Payload des JWS-Token enthalten sein:

- 44 • `scopes` = `scopes`, die bei der Registrierung der Relying Party beim Federation
45 Master angegeben wurden
- 46 • `claims` = `claims`, die bei der Registrierung der Relying Party beim Federation
47 Master angegeben wurden
- 48 • `redirect_uris` = `redirect_uris`, die bei der Registrierung der Relying Party beim
49 Federation Master angegeben wurden

50

51 *Hinweis: Will eine Relying Party den Umfang der vom sektoralen IDP anforderbaren*
52 *scopes oder claims erweitern oder redirect_uris ändern, so müssen diese Änderungen*
53 *über den organisatorischen Registrierungsprozess laufen.*

54 Neu:

55 **AF_10101-01 Bereitstellung von Informationen zu Teilnehmern der Föderation**
56 **durch den Federation Master**

57

58 **Tabelle 1: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der**
59 **Föderation durch den Federation Master"**

Attribute	Bemerkung
Beschreibung	Der Nutzer einer Anwendung der Föderation muss durch die Anwendung autorisiert werden. Im Zuge des Autorisierungsablaufs wird der Nutzer über einen sektoralen Identity Provider authentifiziert. Im Ablauf dieser Autorisierung durch eine Anwendung wird der Federation Master zur Validierung der teilnehmenden Parteien einbezogen. Die Abbildung "Federation Master im Authorization-Flow" zeigt die Schritte in ihrer Abfolge, bei denen eine Kommunikation mit dem Federation Master stattfindet.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen und muss dafür von einem sektoralen Identity Provider der TI authentifiziert werden.
Komponente	<ul style="list-style-type: none"> • Federation Master • Fachdienst der TI • sektoraler Identity Provider

Attribute	Bemerkung
Vorbedingung	<ul style="list-style-type: none"> • Der Fachdienst ist in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt. • Der sektorale Identity Provider ist in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt. • Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>federation_fetch_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein.
Ablauf	<ul style="list-style-type: none"> • Im Ablauf der Nutzung eines Fachdienstes (siehe Abbildung - Flow-Diagramm "Federation Master im Authorization-Flow") findet eine Verzweigung zum Federation Master in dem Fall statt, wenn der Fachdienst das Entity Statement des sektoralen Identity Provider oder wenn der sektorale Identity Provider das Entity Statement des Fachdienstes nicht kennt. • Die unter <code>federation_fetch_endpoint</code> im Entity Statement des Federation Master festgelegte URL MUSS aus dem Internet erreichbar sein. • Für die Abfrage von Informationen zu einem Teilnehmer der Föderation beim Federation Master sendet der anfragende Teilnehmer einen Request an den unter <code>federation_fetch_endpoint</code> im Entity Statement des Federation Master per URL festgelegten Endpunkt. Der Request MUSS die in Tabelle "<i>Teilnehmer Validierung Abfrage - Request Parameter</i>" Parameter umfassen. • Der Federation Master MUSS als Response auf die Anfrage des Fachdienstes ein signiertes JSON Web Token senden. Die Header- und Payload-Attribute des JWS MÜSSEN mindestens die in den Tabellen "<i>Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token</i>" und "<i>Teilnehmer Validierung Abfrage - Response-Header-Attribute des signierten JSON-Web-Token</i>" aufgeführten Attribute enthalten.
Ergebnis	Der anfragende Teilnehmer hat Informationen über den angefragten Teilnehmer erhalten, kann diese entschlüsseln und verwenden.
Akzeptanzkriterien	ML-128451 , ML-128452 ML-136402 , ML-152179
Alternativen	Der Anwendungsfall entfällt, wenn die Teilnehmer sich kennen, eine gegenseitige Validierung bereits früher erfolgt ist und eine erneute Validierung (noch) nicht notwendig ist.

61 4.2 Organisatorische Prozesse am Federation Master

62 Die Anforderung A_22741-01 - Prüfung "scope" von Fachdiensten entfällt und wird durch
63 die neue Anforderung A_25414 ersetzt und um die neue Anforderung A_25415 ergänzt.

64

65 Neu:

66 A_25414 - Prüfung der Entity Statements von Fachdiensten

67 Der Anbieter des Federation Master MUSS einen Prozess etablieren, in dem der Anbieter
68 des Federation Master mindestens täglich die Entity Statements der Fachdienste abfragt
69 und die Werte der in Tabelle "Prüfung der Entity Statements von Fachdiensten"
70 aufgeführten Attribute hinsichtlich der bei der Registrierung hinterlegten Werte prüft.
71 Stimmen die Werte nicht überein, so MUSS der Federation Master die in der Tabelle
72 aufgeführten Maßnahmen treffen.

73 **Tabelle 2 : Prüfung der Entity Statements von Fachdiensten**

Attribut	Abweichung	Auswirkung	Maßnahme
jwtks	Schlüssel, mit der Fachdienst sein Entity Statement signiert, hat sich geändert.	Der im Federation Master hinterlegte Schlüssel ist nicht mehr korrekt, der Vertrauensraum ist ggf. gefährdet.	Einstellen eines Incident und Sperren des Teilnehmers in der Föderation
authority_hints	Die Vertrauenskette hat sich geändert.	Als Vertrauensanker ist nicht mehr der Federation Master eingetragen. Vertrauensraum ist ggf. gefährdet.	Einstellen eines Incident und Sperren des Teilnehmers in der Föderation

Attribut	Abweichung	Auswirkung	Maßnahme
scopes	Der Umfang der vom Fachdienst anfragbaren scopes hat sich geändert.	Hat sich der Umfang, der anfragbaren scopes erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren scopes hat keine negativen Auswirkungen.	Einstellen eines Incidents und Sperren des Teilnehmers in der Föderation
claims	Der Umfang der vom Fachdienst anfragbaren claims hat sich geändert.	Hat sich der Umfang, der anfragbaren claims erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren claims hat keine negativen Auswirkungen.	Einstellen eines Incidents und Sperren des Teilnehmers in der Föderation

Attribut	Abweichung	Auswirkung	Maßnahme
redirect_uris	Der Inhalt der Liste der URLs, an den die vom IDP ausgestellten Identitätsinformationen geschickt werden, hat sich geändert.	Die vom IDP ausgestellten Identitätsinformationen können ggf. an unberechtigte Endpunkte verschickt werden, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdateien.	Einstellen eines Incident und Sperren des Teilnehmers in der Föderation
metadata.openid_relying_party.organization_name	Der Name der Organisation hat sich geändert.	Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident
metadata.openid_relying_party.client_name	Der Name des Fachdienstes (redundant zu metadata:federation_entity:name) hat sich geändert.	Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident
metadata.federation_entity.name	Der Name des Fachdienstes (redundant zu metadata:openid_relying_party:client_name) hat sich geändert.	Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident

74 **[<=]**

75 *Hinweis 1: Das Sperren eines Fachdienstes bedeutet technisch den Ausschluss aus der*
76 *Föderation. Fragt ein sektoraler IDP die Teilnehmerauskunft zu einem gesperrten*
77 *Fachdienst beim Federation Master ab, so antwortet dieser gemäß*
78 *https://openid.net/specs/openid-federation-1.0.html#error_response mit Error Code*
79 *HTTP-401 invalid_client.*

80 *Hinweis 2: Zum Entsperren muss der Fachdienst die Abweichungen in seinem Entity*
81 *Statement korrigieren oder im Fall gewollter Änderungen zur Aktualisierung den*
82 *organisatorischen Registrierungsprozess erneut durchlaufen.*

83 Neu:

- 84 **A_25415 - Entsperrten eines gesperrten Fachdienstes in der TI-Föderation**
85 Hat der Federation Master aufgrund von A_25414 einen Fachdienst in der TI-Föderation
86 gesperrt, so SOLL der Federation Master den Fachdienst ohne weitere Maßnahmen
87 wieder zulassen, wenn dieser die Abweichungen im Entity Statement korrigiert hat. [<=]
88 *Hinweis: Die Anforderung ist als SOLL formuliert. Von dieser Anforderung kann*
89 *abgewichen werden, wenn es begründete Bedenken (z.B. weitere Incidents) gegen die*
90 *Zulassung des Fachdienstes gibt.*
91
92