
C_12721_Anlage

Inhaltsverzeichnis

1	Änderungsbeschreibung.....	2
2	Änderung in gemSpec_IDP_FedMaster.....	3
3	Änderung in gemSpec_IDP_Dienst.....	13
4	Änderungen in Steckbriefen.....	15
4.1	Änderungen in gemProdT_FedMaster.....	15
4.2	Änderungen in gemProdT_IDP-Dienst.....	15

1 Änderungsbeschreibung

Bislang liefert der Federation Master im Datensatz zu den registrierten sekt. IDPs einen Boolean-Wert für pkv. Dadurch konnte die UX z.B. in der eRP-App steuern, ob weitere oder abweichende Angaben bzgl. PKV/GKV zu erfassen sind. Mit Bundespolizei Heilfürsorge wird neben GKV und PKV ein weiteres Segment bzgl. GesundheitsID unterstützt. Die Unterscheidung über einen Boolean ist nicht mehr ausreichend.

Es sind Anpassungen in gemSpec_IDP_FedMaster und ggf. gemSpec_IDP-Dienst notwendig.

- Federation Master
- Es wird in den Datensatz ein neues Feld ktr_type eingefügt mit den möglichen Werten GKV, PKV, HLF
- Es wird das Feld pkv als deprecated markiert
- eRP-Authorization Server
- Mit Umstellung des eRP auf ZETA wird die Schnittstelle zum Abruf der Liste der sekt. IDP auf geänderte information angepasst

2 Änderung in gemSpec_IDP_FedMaster

Es wird Kapitel "3.2 Anwendungsfall - IDP-Liste bereitstellen" wie folgt geändert:

Alt:

AF_10100-01 -Bereitstellung Liste registrierter Identity Provider

Tabelle 1: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider"

Attribute	Bemerkung
Beschreibung	<p>Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Um die Berechtigung sicherzustellen, MUSS der Fachdienst die Authentifizierung des Anwenders gegenüber einem sektoralen Identity Provider veranlassen. Dazu benötigt der Fachdienst die Information vom Anwender, gegen welchen sektoralen Identity Provider er sich identifiziert hat.</p> <p>Der Fachdienst MUSS in seinem Frontend dem Anwender eine Liste, der in der TI registrierten, sektoralen Identity Provider anzeigen. Diese Liste MUSS sich der Fachdienst vom Federation Master erfragen.</p> <p>Der Federation Master MUSS eine API-Schnittstelle bereitstellen, über die ein Fachdienst die Liste, der in der TI registrierten, sektoralen Identity Provider abfragen kann.</p> <p>Jeder Listeneintrag MUSS mindestens diese Informationen enthalten:</p> <ul style="list-style-type: none">• eindeutige issuer-id des sektoralen Identity Provider in der TI-Föderation• Name des sektoralen Identity Provider in lesbarer Form• Logo des sektoralen Identity Provider (wenn vorhanden).• Information, ob es sich um einen sektoralen Identity Provider einer gesetzlichen oder privaten Krankenkasse handelt <p>Der Anwender des Fachdienstes MUSS genau einen sektoralen Identity Provider aus der Liste auswählen. Der Fachdienst kann sich die Zuordnung eines Anwenders zu seinem sektoralen Identity Provider speichern, so dass die Abfrage der Liste beim Federation Master nicht bei jeder Anmeldung des Anwenders wiederholt werden muss.</p>
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung für die Authentifizierung des Anwenders muss dieser auswählen, bei welchem Identity Provider er registriert ist (bei Versicherten - Auswahl der

	Krankenkasse).
Komponenten	<ul style="list-style-type: none"> • Fachdienst der TI • Federation Master
Vorbedingung	<ol style="list-style-type: none"> 1. Der Fachdienst ist in der TI-Föderation registriert, sein Schlüssel ist dem Federation Master bekannt. 2. Es gibt eine Liste in der TI-Föderation registrierter (sektoraler) Identity Provider, deren Schlüssel sind dem Federation Master bekannt. 3. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden. 4. Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>idp_list_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein. 5. Der Federation Master hat die Entity Statements aller registrierten (sektoraler) Identity Provider innerhalb der letzten 24h aktualisiert
Ablauf	<ol style="list-style-type: none"> 1. 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. 2. Der Fachdienst sendet einen Request an die URL, welche im Entity Statement des Federation Master unter dem Attribut <code>idp_list_endpoint</code> benannt ist. Der Federation Master nimmt den Request entgegen. 3. Der Federation Master erstellt eine Liste aller registrierten sektoralen Identity Provider. Die Liste MUSS zu jedem sektoralen Identity Provider diese Attribute enthalten: <ol style="list-style-type: none"> a. Name der Organisation b. URI (iss) des sektoralen Identity Provider c. Logo der Organisation d. Unterstützte Anwendertypen e. Information, ob es sich um den sektoralen Identity Provider einer gesetzlichen oder privaten Krankenkasse handelt 4. 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>Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token</i>" und "<i>Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token</i>" aufgeführten Attribute enthalten.
Ergebnis	<ol style="list-style-type: none"> 1. Der Anwender hat aus der Liste, der in der TI registrierten (sektoralen) Identity Provider denjenigen ausgewählt,



	<p>gegenüber dem er sich zuvor identifiziert hat.</p> <p>2. Der Fachdienst hat alle Informationen, um die Authentifizierung und Autorisierung durchzuführen.</p>
Akzeptanzkriterien	<p> ML-128409 - AF_10100 - Unter idp_list_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response,  ML-143019 - AF_10100 - Payload des JWS-Token enthält Informationen zu jedem registrierten sektoralen Identity Provider der Föderation</p>
Alternativen	<p>Die Fachanwendung kennt (z.B. aus früheren Sitzungen) den sektoralen Identity Provider des Anwenders. In diesem Fall KANN der Anwendungsfall ausgeführt werden.</p>

Tabelle 2: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token

Attribut	Werte / Typ	Beispiel	Anmerkungen
iss	URL	"http://master0815.de"	URL des Federation Master
iat	Alle time-Werte in Sekunden seit 1970, [RFC 7519 Sect.2]	1645398001 = 2022-02-21 00:00:01	Ausstellungszeitpunkt der Liste
exp	Alle time-Werte in Sekunden seit 1970, [RFC 7519 Sect.2]	1645484400 = 2022-02-22 00:00:00 entspricht einer Gültigkeit von 24 Stunden in Bezug auf den Wert in iat	Ablaufzeitpunkt der Gültigkeit der Liste (maximal iat + 24 Stunden)
idp_entity			Der Block <i>idp_entity</i> enthält die Liste der sektoralen Identity Provider und einige Metadaten.
organization_name	String (max. 128 Zeichen)	"IDP 4711"	Der Name des sektoralen Identity Provider zur Anzeige für den Benutzer aus der Definition von " organization_name " im Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Der Wert des Parameters organizatio

			<p>n_name wird bei der täglichen Abfrage des Entity Statement überprüft und ggf. geändert.</p> <p><i>Hinweis: Ist ein sektoraler IDP ggf. temporär nicht erreichbar, so sollte das Herunterladen des Entity Statements über den sektoralen IDP weiter (z.B. stündlich) versucht werden.</i></p>
iss	URI	"https://idp4711.de"	<p>issuer-Wert des jeweiligen sektoralen Identity Provider (URL) - sollte nach Vorgaben der Föderation der Adresse für die Authentisierung entsprechen und wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben.</p>
logo_uri	URI	"https://idp4711.de/logo.png"	<p>Der Parameter "logo_uri" aus dem Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Der Wert des Parameters logo_uri wird bei der täglichen Abfrage des Entity Statement überprüft und ggf. geändert.</p>
user_type_supported	[HCI = Health Care Institution , HP = Health Professional, IP = Insured Person]	"IP"	<p>Der Parameter "user_type_supported" aus dem Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Eine tägliche Aktualisierung über das Entity Statement des IDP ist nicht notwendig.</p>
pkv	Boolean (true/false)	true	<p>Signalisiert, ob der Föderationsteilnehmer Teil der privaten Krankenversicherungen ist.</p>

Folgende Werte müssen Bestandteil des Header der vom Federation Master signierten IDP-Liste sein:

Tabelle 3: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token

Name	Werte	Beispiel	Anmerkungen
alg	ES256	<-	
kid	wie aus jwks im Body des Entity Statement		Identifiziert den verwendeten Schlüssel aus dem jwks im Body des Entity Statement des Federation Master
typ	idp-list+jwt	<-	

【<=,,】



[Neu:](#)

AF_10100-02 -Bereitstellung Liste registrierter Identity Provider

Tabelle 4: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider"

Attribute	Bemerkung
Beschreibung	<p>Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Um die Berechtigung sicherzustellen, MUSS der Fachdienst die Authentifizierung des Anwenders gegenüber einem sektoralen Identity Provider veranlassen. Dazu benötigt der Fachdienst die Information vom Anwender, gegen welchen sektoralen Identity Provider er sich identifiziert hat.</p> <p>Der Fachdienst MUSS in seinem Frontend dem Anwender eine Liste, der in der TI registrierten, sektoralen Identity Provider anzeigen. Diese Liste MUSS sich der Fachdienst vom Federation Master erfragen.</p> <p>Der Federation Master MUSS eine API-Schnittstelle bereitstellen, über die ein Fachdienst die Liste, der in der TI registrierten, sektoralen Identity Provider abfragen kann.</p> <p>Jeder Listeneintrag MUSS mindestens diese Informationen enthalten:</p> <ul style="list-style-type: none"> • eindeutige issuer-id des sektoralen Identity Provider in der TI-Föderation • Name des sektoralen Identity Provider in lesbarer Form • Logo des sektoralen Identity Provider (wenn vorhanden). • Information, um welchen Typ von Kostenträger es sich handelt <p>Der Anwender des Fachdienstes MUSS genau einen sektoralen Identity Provider aus der Liste auswählen. Der Fachdienst kann</p>

	sich die Zuordnung eines Anwenders zu seinem sektoralen Identity Provider speichern, so dass die Abfrage der Liste beim Federation Master nicht bei jeder Anmeldung des Anwenders wiederholt werden muss.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung für die Authentifizierung des Anwenders muss dieser auswählen, bei welchem Identity Provider er registriert ist (bei Versicherten - Auswahl der Krankenkasse).
Komponenten	<ul style="list-style-type: none"> • Fachdienst der TI • Federation Master
Vorbedingung	<ol style="list-style-type: none"> 1. Der Fachdienst ist in der TI-Föderation registriert, sein Schlüssel ist dem Federation Master bekannt. 2. Es gibt eine Liste in der TI-Föderation registrierter (sektoraler) Identity Provider, deren Schlüssel sind dem Federation Master bekannt. 3. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden. 4. Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>idp_list_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein. 5. Der Federation Master hat die Entity Statements aller registrierten (sektoraler) Identity Provider innerhalb der letzten 24h aktualisiert
Ablauf	<ol style="list-style-type: none"> 1. 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. 2. Der Fachdienst sendet einen Request an die URL, welche im Entity Statement des Federation Master unter dem Attribut <code>idp_list_endpoint</code> benannt ist. Der Federation Master nimmt den Request entgegen. 3. Der Federation Master erstellt eine Liste aller registrierten sektoralen Identity Provider. Die Liste MUSS zu jedem sektoralen Identity Provider diese Attribute enthalten: <ol style="list-style-type: none"> a. Name der Organisation b. URI (iss) des sektoralen Identity Provider c. Logo der Organisation d. Unterstützte Anwendertypen e. Information, um welchen Typ von Kostenträger es sich handelt

	4. 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 "Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token" und "Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token" aufgeführten Attribute enthalten.
Ergebnis	<ol style="list-style-type: none"> 1. Der Anwender hat aus der Liste, der in der TI registrierten (sektoralen) Identity Provider denjenigen ausgewählt, gegenüber dem er sich zuvor identifiziert hat. 2. Der Fachdienst hat alle Informationen, um die Authentifizierung und Autorisierung durchzuführen.
Akzeptanzkriterien	 ML-128409 - AF_10100 - Unter idp_list_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response ,  ML-143019 - AF_10100 - Payload des JWS-Token enthält Informationen zu jedem registrierten sektoralen Identity Provider der Föderation
Alternativen	Die Fachanwendung kennt (z.B. aus früheren Sitzungen) den sektoralen Identity Provider des Anwenders. In diesem Fall KANN der Anwendungsfall ausgeführt werden.

46
47

Tabelle 5: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token

Attribut	Werte / Typ	Anmerkungen
iss	string, URL nach [RFC1738]	URL des Federation Master
iat	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]	Ausstellungszeitpunkt der Liste
exp	number, Alle time-Werte in Sekunden seit 1970, [RFC7519#section-2]	Ablaufzeitpunkt der Gültigkeit der Liste
idp_entity		Der Block <i>idp_entity</i> enthält die Liste der sektoralen Identity Provider und einige Metadaten.
organization_name	string (gemäß [OpenID-Federation "Informational Metadata Extensions"] - organization_name) Wertebereich: <code>^[à-üÄ-Üßw\ \-\.\+*V]</code>	Der Name des sektoralen Identity Provider zur Anzeige für den Benutzer wird aus dem Parametersorganization_name im Entity Statement des sektoralen Identity Provider ermittelt.

	{1,128}\$	
iss	string, URL nach [RFC1738]	Der issuer-Wert des jeweiligen sektoralen Identity Provider (URL) entspricht dem Parameters iss im Entity Statement des sektoralen Identity Provider.
logo_uri	URI zulässige Formate: PNG	Der Wert für "logo_uri" wird aus dem Parameters logo_uri im Entity Statement des sektoralen Identity Provider ermittelt.
user_type_supported	[string] zulässiger Wert: "IP" (Insured Person)	Der Wert für "user_type_supported" wird aus dem Parameters user_type_supported im Entity Statement des sektoralen Identity Provider ermittelt.
pkv (deprecated)	boolean, Wertebereich: true/false	Signalisiert, ob der Föderationsteilnehmer Teil der privaten Krankenversicherungen ist. Der Parameter entfällt nach vollständiger Umstellung auf ktr_type nach einer Karenzzeit in einer weiteren Stufe..
ktr_type	[string], Wertebereich: "pkv", "gkv", "hlf"	Signalisiert, welcher Typ Kostenträger den sektoralen IDP in der TI-Föderation stellt. <ul style="list-style-type: none"> • gkv - gesetzliche Krankenversicherungen • pkv - private Krankenversicherungen • hlf - Heilfürsorge (Bundespolizei)

Folgende Werte müssen Bestandteil des Header der vom Federation Master signierten IDP-Liste sein:

Tabelle 6: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen
alg	string, zulässiger Wert "ES256"	

kid	string UUID7-Format [RFC9562#name-uuid-version-7]	Identifiziert das federation_entity_signing_key des Federation Master. Der Schlüssel kann aus dem jwks im Body des Entity Statement des Federation Master ermittelt werden.
typ	idp-list+jwt	

53 **【<=,IDP_FedMaster,funkt. Eignung: Test Produkt/FA】**

54
55 [Alt:](#)

56 **ML-143019 -AF_10100 - Payload des JWS-Token enthält Informationen zu jedem**
 57 **registrierten sektoralen Identity Provider der Föderation**

58 Der Payload des JWS-Token enthält zu jedem in der Föderation registrierten sektoralen
 59 Identity Provider die Informationen:

- 60 • Organisationsname
- 61 • URL, unter welcher das Logo der Organisation abrufbar ist
- 62 • URI des sektoralen Identity Provider, welcher dem Identifier (iss) des sektoralen
- 63 Identity Provider entspricht
- 64 • Liste der supporteten Usertype
- 65 • Information darüber ob der sektoralen Identity Provider für gesetzliche oder
- 66 privatversicherte Patienten verwendet wird

67 **【<=】**

68 [Neu:](#)

69 **ML-190096 -AF_10100 - Payload des JWS-Token enthält Informationen zu jedem**
 70 **registrierten sektoralen Identity Provider der Föderation**

71 Der Payload des JWS-Token enthält zu jedem in der Föderation registrierten sektoralen
 72 Identity Provider die Informationen:

- 74 • Organisationsname
- 75 • URL, unter welcher das Logo der Organisation abrufbar ist
- 76 • URI des sektoralen Identity Provider, welcher dem Identifier (iss) des sektoralen
- 77 Identity Provider entspricht
- 78 • Liste der supporteten Usertype
- 79 • Information, um welchen Typ von Kostenträger es sich handelt

80 **【<=】**

3 Änderung in gemSpec_IDP_Dienst

Es wird Kapitel "5.1.4 Auswahlliste der sektoraler Identity Provider für den Nutzer" wie folgt geändert:

Alt:

A_23681-03 -Bereitstellung einer Liste der sektoralen Identity Provider innerhalb der Föderation

Der IDP-Dienst MUSS gemäß [gemSpec_IDP_FD#AF_10116] unter einer dedizierten URL eine Liste der in der TI-Föderation registrierten sektoralen Identity Provider bereitstellen. Diese Liste muss der IDP-Dienst unter der URL, welche im Entity Statement des Federation Master unter dem Claim idp_list_endpoint angegeben ist, laden (siehe [A_10100-*]).

Der IDP-Dienst MUSS diese Daten verwenden, um für jeden sektoralen IDP dieser Liste einen Eintrag für die eigene, bereitzustellende Liste mit folgenden Daten zu erstellen:

Datum	Erläuterung	Anmerkung
idp_name	Name der Krankenkasse, zur Anzeige in der E-Rezept-App (max. 128 Zeichen)	Entspricht dem Wert in idp_entity.organization_name im Listeneintrag der Liste des Federation Master.
idp_iss	URL des Claim iss des sektoralen IDP der Föderation (maximal 2000 VSCAHR)	Entspricht dem Wert in idp_entity.iss im Listeneintrag der Liste des Federation Master.
idp_pkv	Boolean False für gesetzliche Krankenversicherungen True für private Krankenversicherungen	Entspricht dem Wert in idp_entity.pkv im Listeneintrag der Liste des Federation Master.
idp_logo	Logo zur Anzeige in der Auswahlliste	Entspricht dem Wert in idp_entity.logo_uri im Listeneintrag der Liste des Federation Master.

[<=,,]

Neu:

A_23681-04 -Bereitstellung einer Liste der sektoralen Identity Provider innerhalb der Föderation

Der IDP-Dienst MUSS gemäß [gemSpec_IDP_FD#AF_10116] unter einer dedizierten URL eine Liste der in der TI-Föderation registrierten sektoralen Identity Provider bereitstellen. Diese Liste muss der IDP-Dienst unter der URL, welche im Entity Statement des Federation Master unter dem Claim idp_list_endpoint angegeben ist, laden (siehe [A_10100-*]).

Der IDP-Dienst MUSS diese Daten verwenden, um für jeden sektoralen IDP dieser Liste einen Eintrag für die eigene, bereitzustellende Liste mit folgenden Daten zu erstellen:

Datum	Erläuterung	Anmerkung
idp_name	Name der Krankenkasse, zur Anzeige in der E-Rezept-App (max. 128 Zeichen)	Entspricht dem Wert in idp_entity.organization_name im Listeneintrag der Liste des Federation Master.
idp_iss	URL des Claim iss des sektoralen IDP der Föderation (maximal 2000 VSCAHR)	Entspricht dem Wert in idp_entity.iss im Listeneintrag der Liste des Federation Master.
idp_pkv (deprecated)	Boolean False für gesetzliche Krankenversicherungen True für private Krankenversicherungen	Entspricht dem Wert in idp_entity.pkv im Listeneintrag der Liste des Federation Master. Der Parameter entfällt nach vollständiger Umstellung auf ktr_type nach einer Karenzzeit in einer weiteren Stufe.
idp_ktr	String des Kosträgertyps, zur Steuerung von Kostenträger spezifischen Funktionen in der E-Rezept-App Der Wert kann folgende Ausprägungen haben: <ul style="list-style-type: none">• gkv - gesetzliche Krankenkasse• pkv - private Krankenkasse• hlf - Heilfürsorge	Entspricht dem Wert in idp_entity.ktr_type im Listeneintrag der Liste des Federation Master.
idp_logo	Logo zur Anzeige in der Auswahlliste	Entspricht dem Wert in idp_entity.logo_uri im Listeneintrag der Liste des Federation Master.

【<=,IDP-D,funkt. Eignung: Herstellererklärung】

4 Änderungen in Steckbriefen

4.1 Änderungen in gemProdT_FedMaster

Tabelle 7: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
AF_10100-01	Bereitstellung Liste registrierter Identity Provider	gemSpec_IDP_FedMaster
AF_10100-02	Bereitstellung Liste registrierter Identity Provider	gemSpec_IDP_FedMaster

4.2 Änderungen in gemProdT_IDP-Dienst

Tabelle 8: Anforderungen zur funktionalen Eignung "Herstellereklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23681-03	Bereitstellung einer Liste der sektoralen Identity Provider innerhalb der Föderation	gemSpec_IDP_Dienst
A_23681-04	Bereitstellung einer Liste der sektoralen Identity Provider innerhalb der Föderation	gemSpec_IDP_Dienst