
C_12207 - E-Rezept: Standardkonforme Darstellung des Authentifizierungsverfahren im ACCESS_TOKEN

Inhaltsverzeichnis

1 Änderungsbedarf.....	2
2 Änderungsbeschreibung.....	3
2.1 Änderung in gemSpec_IDP_Dienst.....	3
2.2 Änderung in gemSpec_FD_eRp.....	5

1 Änderungsbedarf

Nutzer, welche Zugriff auf den E-Rezept-Fachdienst erhalten wollen, müssen sich über den IDP-Dienst authentifizieren. Der IDP-Dienst stellt nach erfolgreicher Authentifizierung ein ACCESS_TOKEN aus. Dieses ACCESS_TOKEN muss beim Aufruf des E-Rezept-Fachdienst als Nachweis der Zugriffsautorisierung mitgegeben werden.

Der IDP-Dienst hat für den Authentifizierungsablauf eine Anpassung an den OIDC-Standard vorgesehen (siehe Änderungseintrag "C_12182 Anpassung ID Token an Standard").

Folgende Änderungen dienen dazu die Anpassungen auch im ACCESS_TOKEN abzubilden.

Dieser Änderungseintrag ändert die technische Umsetzung von Änderungseintrag "C_11984 E-Rezept: Nutzung der Akzeptanzfeatures GesundheitsID für E-Rezept".

2 Änderungsbeschreibung

2.1 Änderung in gemSpec_IDP_Dienst

Der E-Rezept Authorization Server stellt nach der Nutzerauthentifizierung durch den IDP dem eRP-FdV ein (eigenes) ID Token (Access-Token) aus. Die Festlegungen zum Inhalt sind spezifiziert in:

alt:

A_22271-02 - Befüllen der Claims "display_name", "organizationName", "professionOID", "idNummer", "organizationIK", "acr" und "amr" nach Bestätigung durch einen sektoralen Identity Provider

Der Token-Endpunkt MUSS benötigte Attribute in Claims für das auszustellende ACCESS_TOKEN und das ID_TOKEN ausschließlich aus den entsprechenden Claims des ID_TOKEN des sektoralen Identity Provider beziehen.

Der Claim amr MUSS entsprechend des ursprünglich zur Authentisierung verwendeten Authentisierungsmittels belegt werden.

Tabelle 1: TAB_IDP_DIENST_0007 Befüllung der Attribute nach Bestätigung durch einen sektoralen Identity Provider

Attribute	Versicherte
display_name	Vollständiger Name des Versicherten, entspricht dem claim urn:telematik:claims:display_name aus dem vom sektoralen IDP ausgestellten ID-Token
given_name	Vorname des Versicherten, entspricht dem claim urn:telematik:claims:given_name aus dem vom sektoralen IDP ausgestellten ID-Token
family_name	Familienname des Versicherten, entspricht dem claim urn:telematik:claims:family_name aus dem vom sektoralen IDP ausgestellten ID-Token
organizationName	Herausgeber-ID (Institutionskennzeichen), entspricht dem claim urn:telematik:claims:organization aus dem vom sektoralen IDP ausgestellten ID-Token
professionOID	ProfessionOID, entspricht dem claim urn:telematik:claims:profession aus dem vom sektoralen IDP ausgestellten ID-Token. Der Wert ist immer 1.2.276.0.76.4.49 .
idNummer	KVNR, entspricht dem claim urn:telematik:claims:id aus dem vom sektoralen IDP ausgestellten ID-Token
organizationIK	Herausgeber-ID (Institutionskennzeichen), entspricht dem claim urn:telematik:claims:organization aus dem vom

	sektoralen IDP ausgestellten ID-Token
amr	"mfa"
acr	"gematik-ehealth-loa-high"

[<=, IDP-D, funkt. Eignung: Test Produkt/FA]

neu:

A_22271-04 - Befüllen der Claims "display_name", "organizationName", "professionOID", "idNummer", "organizationIK", "acr" und "amr" nach Bestätigung durch einen sektoralen Identity Provider

Der Token-Endpunkt MUSS benötigte Attribute in Claims für das auszustellende ACCESS_TOKEN und das ID_TOKEN ausschließlich aus den entsprechenden Claims des ID_TOKEN des sektoralen Identity Provider beziehen.

Tabelle 2: TAB_IDP_DIENST_0007 Befüllung der Attribute nach Bestätigung durch einen sektoralen Identity Provider

Attribute	Versicherte
display_name	Vollständiger Name des Versicherten, entspricht dem Claim urn:telematik:claims:display_name aus dem vom sektoralen IDP ausgestellten ID Token
given_name	Vorname des Versicherten, entspricht dem Claim urn:telematik:claims:given_name aus dem vom sektoralen IDP ausgestellten ID Token
family_name	Familiennamen des Versicherten, entspricht dem Claim urn:telematik:claims:family_name aus dem vom sektoralen IDP ausgestellten ID Token
organizationName	Herausgeber-ID (Institutionskennzeichen), entspricht dem claim urn:telematik:claims:organization aus dem vom sektoralen IDP ausgestellten ID Token
professionOID	ProfessionOID, entspricht dem Claim urn:telematik:claims:profession aus dem vom sektoralen IDP ausgestellten ID Token. Der Wert ist immer 1.2.276.0.76.4.49 .
idNummer	KVNR, entspricht dem Claim urn:telematik:claims:id aus dem vom sektoralen IDP ausgestellten ID Token
organizationIK	Herausgeber-ID (Institutionskennzeichen), entspricht dem Claim urn:telematik:claims:organization aus dem vom sektoralen IDP ausgestellten ID Token

amr	amr-Wert aus dem ID-Token des sektoralen IDP
acr	acr-Wert aus dem ID Token des sektoralen IDP ("gematik-ehealth-loa-high" oder "gematik-ehealth-loa-substantial")
urn:telematik:auth:consent	urn:telematik:auth:consent aus dem ID Token des sektoralen IDP ("loa-substantial")

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

2.2 Änderung in gemSpec_FD_eRp

alt:

A_19439-03 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke

Der E-Rezept-Fachdienst MUSS die Authentisierungsstärke der Nutzerauthentisierung anhand der Kombinationen von Attributen gemäß TAB_eRPFD_027 des im HTTP-Header "Authorization" übergebenen ACCESS_TOKEN feststellen und ACCESS_TOKEN mit anderen als den zulässigen Kombinationen mit dem HTTP-Status-Code 401 ablehnen.

Tabelle 3 : TAB_eRPFD_027 Authentifizierungsstärke

professionOID	acr	amr
beliebig	gematik-ehealth-loa-high	beliebig
oid_versicherter	gematik-ehealth-loa-substantial	urn:telematik:auth:mEW

【<=, eRp_FD, Sich.techn. Eignung: Produktgutachten】

neu:

A_19439-04 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke

Der E-Rezept-Fachdienst MUSS die Authentisierungsstärke der Nutzerauthentisierung anhand der Kombinationen von Attributen gemäß TAB_eRPFD_027 des im HTTP-Header "Authorization" übergebenen ACCESS_TOKEN feststellen und ACCESS_TOKEN mit anderen als den zulässigen Kombinationen mit dem HTTP-Status-Code 401 ablehnen.

Tabelle 4 : TAB_eRPFD_027 Authentifizierungsstärke

professionOID	acr	urn:telematik:auth:consent
beliebig	gematik-ehealth-loa-high	beliebig
oid_versicherter	gematik-ehealth-loa-substantial	loa-substantial

【<=, eRp_FD, Sich.techn. Eignung: Produktgutachten】

Das Attribut urn:telematik:auth:consent ist optional im ACCESS_TOKEN.

