

C_12817_Anlage

Überarbeitung des Kapitels 3.17.3, um generisch JWT-Bearer-Token zu adressieren

3.17.3 Anforderungen an den Authorization Service für die Authentisierung über JWT Bearer Token

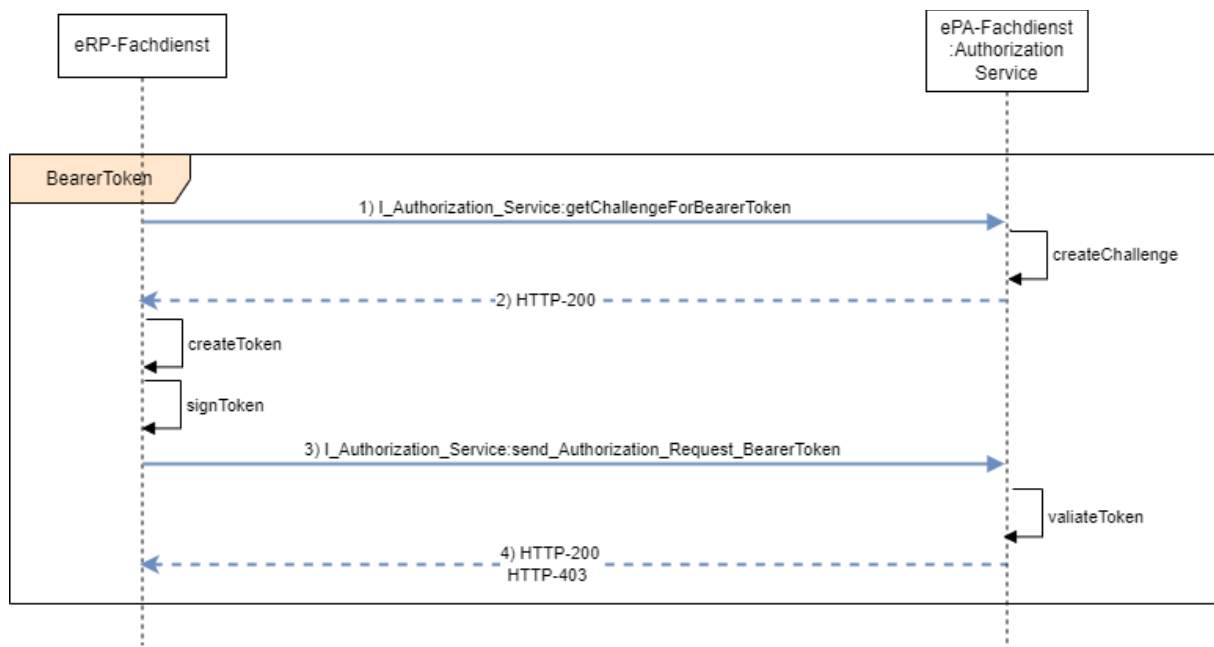


Abbildung1: Ablauf der Authentisierung über JWT Bearer Token am Beispiel eRP-FD

A_25165-03 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_25165-03

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle I_Authorization_Service durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Tabelle 36 : JWT Bearer Token eRP mit den Mindest-Inhalten

Part	Claim Name	Claim	Anmerkung
Protected Header			

	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

[<=]

A_29875 -Authorization Service: JWT Bearer-Token des Forschungsdatenzentrums

Der Authorization Service MUSS sicherstellen, dass die Authentifizierung des Forschungsdatenzentrums über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Tabelle1 : JWT Bearer Token FDZ mit den Mindest-Inhalten

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Kr
	"sub"	Telematik-ID des Forschungsdatenzentrums	

34 【<=,EPA-Authorization-Service,funkt. Eignung: Herstellererklärung, funkt. Eignung: Test
35 Produkt/FA】

36
37 Das Signaturzertifikat zu "x5c" (AUT-Zertifikat des Forschungsdatenzentrums) kommt aus
38 der Komponenten-PKI der TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve
39 brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und
40 nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß
41 [RFC7515] zu erstellen.