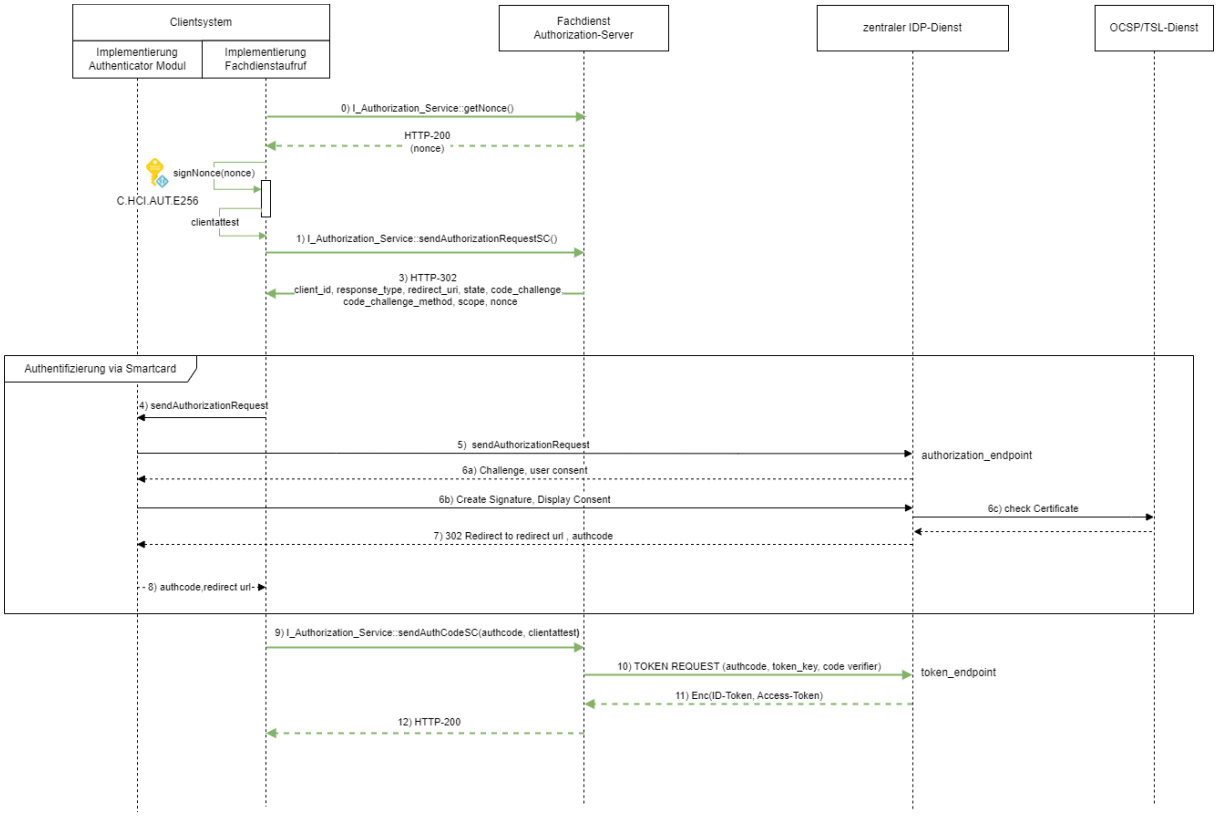
Änderung in gemILF_PS_ePA

Aktualisierung von Abbildung 1: Detaillierter Nachrichten-Flow für die Nutzerauthentifizierung mit dem IDP-Dienst



Alt:

A_24944 - Anfrage des "AUTHORIZATION_CODE" für ein "ID_TOKEN"
Das Primärsystem MUSS den Antrag zum "AUTHORIZATION_CODE" für ein "ID_TOKEN" beim Authorization-Endpunkt (URI_AUTH) in Form eines HTTP/1.1 GET Request stellen und dabei die folgenden Attribute aus der send_Authorization_Request Antwort des Authorization Server übermitteln:

- "response_type"
- "scope"
- "nonce"
- "client_id"
- "redirect_uri"
- "code_challenge" (Hashwert des "code_verifier") [RFC7636 # section-4.2]
- "code_challenge_method" HASH-Algorithmus (S256) [RFC7636 # section-4.3]

[<=]

Neu:

A_24944-01 - Anfrage des "AUTHORIZATION_CODE" für ein "ID_TOKEN"
Das Primärsystem MUSS in Form eines HTTP/1.1 GET AuthorizationRequest beim Authorization-Endpunkt (URI_AUTH) den Antrag zum Erhalt eines "AUTHORIZATION_CODE" für ein "ID_TOKEN" stellen. Dabei übermittelt es die folgenden Attribute, die aus der Response von send_Authorization_Request stammen:

- "response_type"
- "scope"
- "nonce"
- "client_id"
- "redirect_uri"
- "code_challenge" (Hashwert des "code_verifier") [RFC7636 # section-4.2]
- "code_challenge_method" HASH-Algorithmus (S256) [RFC7636 # section-4.3]
- "state"

[<=]

Änderung in gemSpec_Aktensystem_ePAfueralle

Änderung in Kapitel 3.15 Zusätzliche Anforderungen an den Authorization Service

Die Abbildung 2: "Ablauf der Authentifizierung von Versicherten über sektorale IDPs und Leistungserbringern über den Smartcard IDP" wird entfernt und statt dessen für die einzelnen Anwendungsfälle jeweils neue, aktualisierte Abbildungen in den Unterkapiteln eingefügt.

Änderung in Kapitel 3.15.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)

Neu: (eingefügt oberhalb A_24877)

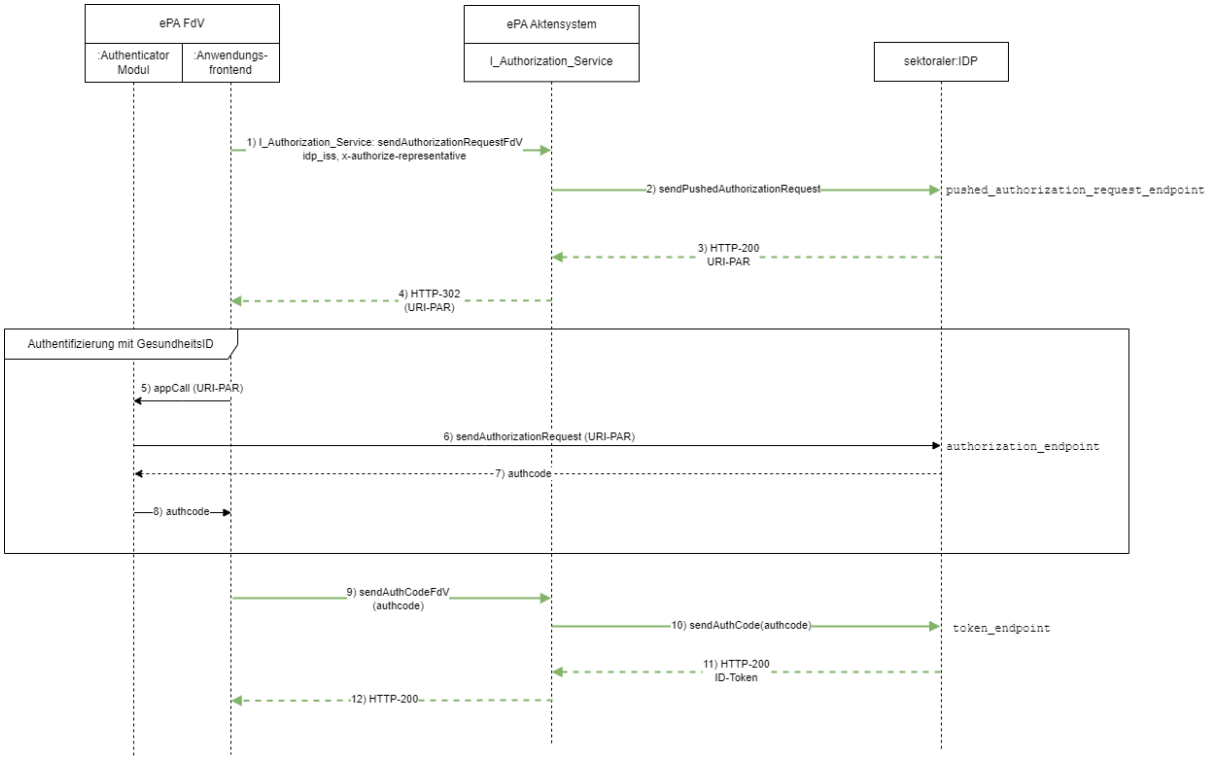


Abbildung: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

Änderung in Kapitel 3.15.2 Anforderungen an den Authorization Service für die Authentisierung mit SMC-B

Neu: (eingefügt oberhalb A_24880)

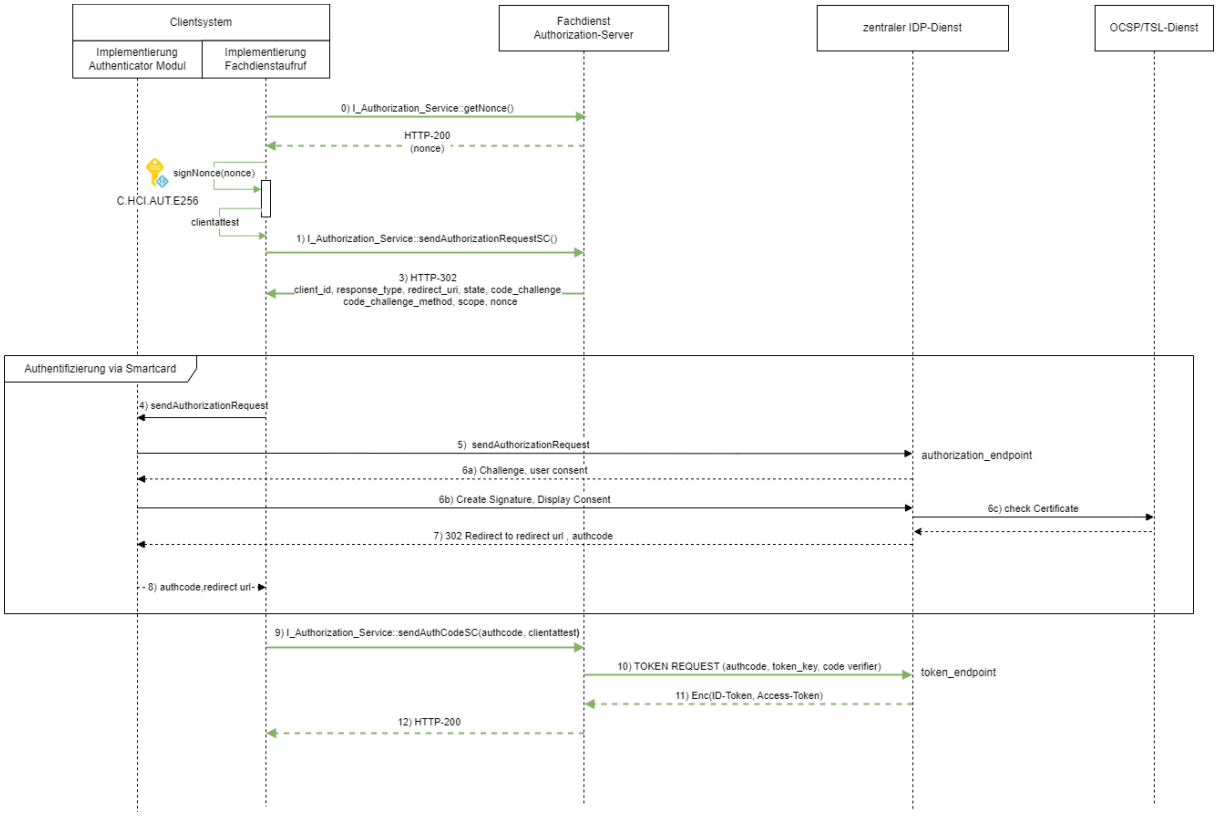


Abbildung: Abbildung: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

A_24880 entfällt (abgedeckt durch API)

A_24805 entfällt (redundant zu A_24717)

neu:

A_25444 - Authorization Service - JWT Client Attestation
Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen , dass das übermittelte JWT der Client Attesttierung mindestens die folgenden Inhalte aufweist.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	

Part	Claim Name	Claim	Anmerkung
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"nonce"	Nonce aus einer `getNonce` Operation	siehe [I_Authorization_Service]

[<=]

Änderung in Kapitel 3.15.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes

Neu: (eingefügt oberhalb A_25165)

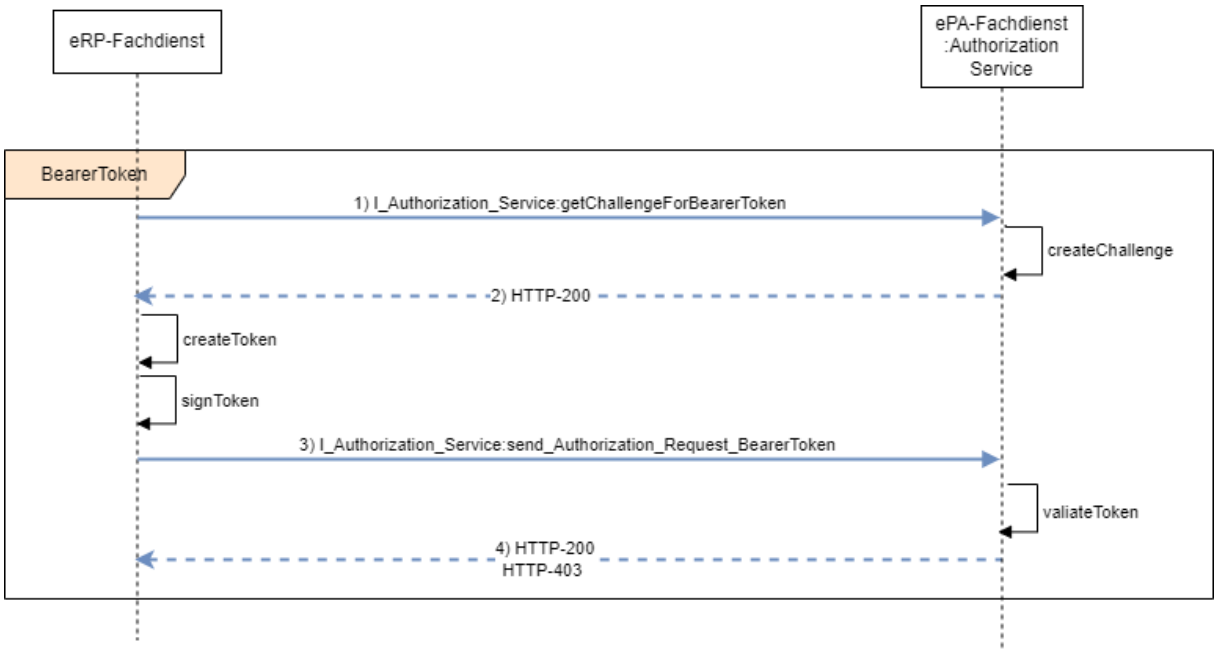


Abbildung: Ablauf der Authentisierung des E-Rezept-Fachdienste

A_24165 wird geändert

alt:

A_25165 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes
Der Authorization Service MUSS bei der Authentifizierung des E-Rezept-Fachdienstes prüfen, dass das übermittelte JWT (vgl. [gemspec_Krypt#A_ 24658-*] mit mindestens folgenden Inhalten und den in A_24658-* definierten Inhalten erfolgt:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"iss"	URI des Token Ausstellers (issuer)	https://erezept.fachdienst.de
	"sub"	Identifier (Telematik-ID)	9-E_Rezept_Fachdienst
	"iat"	Zeitstempel Ausgabezeitpunkt	1705674544
	"exp"	Verfalldatum, = "iat" + 20 min	1705675744
	"oid"	professionOid	1.2.276.0.76.4.258 (vgl. [gemSpec_OID#GS-A_4446-*] oid_erp-vau)
	"validTo"	Ende der Gültigkeit (tagesgenau)	2025-06-30

[<=]

neu:

A_25165-01 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes
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.

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	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	
	"oid"	oid_erp-vau (1.2.276.0.76.4.25)	fester Wert gemäß [gemSpec_OID]

[<=]

Änderung in Kapitel 3.18.1 Übersicht der Schnittstellen des Aktensystems

© gematik – öffentlich_Entwurf

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
...	
I_Authorization_Service	
Schnittstelle der Autorisierung für den Login	
`getFHIRVZDtoken`	Diese Operation bezieht das search-access-token für den Zugriff auf den FHIR VZD vom Aktensystem
`getNonce`	Diese Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung
`sendAuthorizationRequestSC`	Diese Operation initiiert die Authentifizierung eines Leistungserbringers
`sendAuthCodeSC`	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
`getChallengeForBearerToken`	Die Operation erzeugt eine gültige Challenge für ein JWT Bearer token
`sendAuthorizationRequestBearerToken`	Diese Operation initiiert die Authentifizierung über Bearer Token
`sendAuthorizationRequestFdV`	Diese Operation initiiert die Authentifizierung eines ePA-FdV
`sendAuthCodeFdV`	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
`logoutFdV`	Diese Operation beendet aktiv die Sitzung
....	

Änderung in I_Authorization_Service.yaml

siehe **https://github.com/gematik/ePA-Basic/tree/ePA-3.0.1**