Änderung in I_Authorization_Service.yaml

sendAuthorizationRequestFdV

- x-device-id und x-device-token sind missverständlich und werden ersetzt durch http-header Parameter x-authorize-representative (true/false); Parameter ist true, wenn eine Authentisierung im Anwendungsfall "Vertretung am fremden FdV verwalten" gefordert wird

Änderung in gemSpec_ePA_FdV

Redaktionelle Änderung! - keine Suffix-Afo für folgende Anpassungen:

Der Aufruf der Operationen des I_Authorization_Service werden
in gemSpec_ePA_FdV konsistent übernommen, d.h.

1. send_Authorization_Request wird ersetzt durch sendAuthorizationRequestFdV in:
   - Tabelle: Schnittstellen des ePA-Aktensystems
   - A_24830 und informativer Text darunter
   - 6.1.3 Authentisierung
2. send_authcode wird ersetzt durch sendAuthCodeFdV
   - Tabelle: Schnittstellen des ePA-Aktensystems
   - A_15292-06
   - A_24831 und informativer Text darunter
   - 6.1.3 Authentisierung
3. logout wird ersetzt durch logoutFdV
   - A_24759

Neue Anforderung:

A_25227 - ePA-Frontend des Versicherten: Login - registriertes Gerät
Falls das verwendete Gerät des Nutzers bereits registriert ist, MUSS das ePA-Frontend des Versicherten im Anwendungsfall "Login User" diese Registrierungsdaten bei der Kommunikation mit dem Authorization Service verwenden gemäß [I_Authorization_Service].**[<=]**

enfällt:

A_24405 - ePA-Frontend des Versicherten: Vertretung am fremden FdV verwalten - Authentisierung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung am fremden FdV verwalten" auf dem Gerät des zukünftigen Vertreters die Authentisierung des zu Vertretenden am IdP mit GesundheitsID durch Angabe von AUTHORIZE_REPRESENTATIVE verlangen.**[<=]**

und wird abgelöst durch:

A_24405-01 - ePA-Frontend des Versicherten: Vertretung am fremden FdV verwalten - Authentisierung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung am fremden FdV verwalten" auf dem Gerät des zukünftigen Vertreters die Authentisierung des zu Vertretenden am IdP mit GesundheitsID ohne Gerätebindung verlangen gemäß [I_Authorization_Service].**[<=]**

© gematik – öffentlich_Entwurf

Änderung in gemSpec_Aktensystem_ePAfueralle

Redaktionelle Änderung! - keine Suffix-Afo für folgende Änderungen:

Der Aufruf der Operationen des I_Authorization_Service werden in gemSpec_Aktensystem_ePAfueralle konsistent übernommen, d.h.

1. send_authcode wird ersetzt durch sendAuthCodeFdV
   - A_24914
2. send_AuthCode_SC wird ersetzt durch sendAuthCodeSC
   - A_24880

Eingangsparameter DeviceID = AUTHORIZE_REPRESENTATIVE wird ersetzt durch `x-authorize-representative=True`

entfällt:

A_24878 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Falls der Eingangsparameter DeviceID = AUTHORIZE_REPRESENTATIVE der Operation `I_Authorization_Service::send_Authorization_Request_FdV` gesetzt ist MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:eGK` und `urn:telematik:auth:eID` belegt sein, um sicherzustellen, dass sich der Nutzer nur entweder über nPA+PIN oder eGK+PIN authentifizieren darf. **[<=]**

und wird abgelöst durch:

A_24878-01 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Falls der Eingangsparameter `x-authorize-representative=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:eGK` und `urn:telematik:auth:eID` belegt sein, um sicherzustellen, dass sich der Nutzer nur entweder über nPA+PIN oder eGK+PIN authentifizieren darf. **[<=]**

entfällt:

A_24937 - Authorization Service - Einschränkung bei AUTHORIZE_REPRESENTATIVE
Der Authorization Service MUSS sicherstellen, dass ein mit AUTHORIZE_REPRESENTATIVE authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält.**[<=]**

und wird abgelöst durch:

A_24937-01 - Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Der Authorization Service MUSS sicherstellen, dass ein mit `x-authorize-representative=True` authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält.**[<=]**

entfällt:

© gematik – öffentlich_Entwurf

A_24804 - Authorization Service - Prüfung auf registriertes Gerät
Der Authorization Service MUSS bei der Authentifizierung eines Versicherten prüfen, ob die in der Operation `I_Authorization_Service::sendAuthCodeFdV` übergebene DeviceID auf den authentifizierten Nutzer registriert und verifiziert ist, wenn der Wert `DeviceID` nicht `AUTHORIZE_REPRESENTATIVE` ist.**[<=]**

und wird abgelöst durch:

A_24804-01 - Authorization Service - Prüfung auf registriertes Gerät
Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf `I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt.**[<=]**

entfällt:

A_24936 - Authorization Service - keine Geräteregistrierung bei AUTHORIZE_REPRESENTATIVE
Falls DeviceID = AUTHORIZE_REPRESENTATIVE übergeben wird MUSS der Authorization Service sicherstellen, dass keine Geräteregistrierung erfolgt.**[<=]**

und wird abgelöst durch:

A_24936-01 - Authorization Service - keine Geräteregistrierung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Falls der Eingangsparameter `x-authorize-representative=True` gesetzt ist MUSS der Authorization Service sicherstellen, dass keine Geräteregistrierung erfolgt.**[<=]**

entfällt:

A_24915 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht verifiziert
Falls eine nicht verifizierte DeviceID in der Operation send_AuthCode übergeben wurde MUSS der Authorization Service die Operation mit HTTP-Status 403 (Forbidden) mit ErrorCode = "pendingDevice" abbrechen.**[<=]**

und wird abgelöst duch:

A_24915-01 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt
Falls eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.**[<=]**

© gematik – öffentlich_Entwurf