

C_12086_Anlage

Änderung in gemSpec_Aktensystem_ePAfueralle

alt:

A_25717-02 - Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) an durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
redirect_uri	Inhalt des optionalen Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], andernfalls der Wert <Location Authorization Service>/epa/authz/<version>/send_authcode_fdv	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene redirect_uri verwenden [sendAuthorizationRequestFdV in I_Authorization_Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.

[<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten]

neu:

A_25717-03 - Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) an durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter"	Notwendige Scopes für den Zugriff für die Autorisierung von

		Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
redirect_uri	Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], andernfalls eine herstellerspezifische Standard-redirect_uri.	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene redirect_uri verwenden [sendAuthorizationRequestFdV in I_Authorization_Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.

Sich.techn. Eignung: Produktgutachten, <=

Änderung in I_Authorization_Service.yaml

version 1.5.0 -> 1.5.1

sendAuthorizationRequestFdV

alt: -----

description: |

Sends an authorization request to the authorization service.

****Client**:** </br>

A client shall use parameter _x-authorize_representative_ for the "Authorize Representative" use case,

a login of a user on not owned device for representative entitlement only.

The _x-authorize-representative_ parameter will force an authentication of the user with egK + pin only and limit the possible operations to entitlement management only.

*A client shall use the returned redirect url to invoke the authenticator.
*

A client shall use parameter _x-authorize-validation_ for a login of a validation identity (e.g. "Prüfkarte eGK"),

forcing the authorization service to request an authentication at the identity provider in guest mode (eGK + pin).

A client shall use the returned redirect url to invoke the authenticator.

****Provider**:** </br>

The authorization service shall send a pushed authorization request (PAR) to the IDP (see: find more details).

The _redirect_uri_ parameter of the PAR shall be set to <Location Authorization Service>/epa/authz/<version>/send_authcode_fdv

when operation parameter _x-redirecturi_ is not present, else the content of _x-redirecturi_ shall be used (according to A_25717-*).

The authorize representative situation (_x-authorize-representative_ == _true_) shall be kept for the subsequent

sendAuthCodeFdV and device management operations.

For the `_x-authorize-representative_` and the `_x-authorize-validation_` case the PAR for the IDP shall include:

- `amr = urn:telematik:auth:guest:eGK`

`_x-authorize-representative_` and `_x-authorize-validation_` both should not be set to `_true_` at the same time.

The authorization service' state value and `clientid` used for the PAR shall occur in the URI-PAR response of the IDP.

Conditions	Status code	Error code	Remarks
Successful operation	302		
Request does not match schema	400	<code>malformedRequest</code>	also if both " <code>x-authorize</code> "-parameters are set to <code>_true_</code>
Invalid request	403	<code>invalAuth</code>	includes any error of Authorization Service and IDP which is not mapped to 500 internal Server error
state or <code>clientid</code> value mismatch	403	<code>invalData</code>	returned URI-PAR does not contain expected state or <code>clientid</code> value
unregistered redirecturi	403	invalRedir	redirecturi (e.g. <code>_x-redirecturi_</code>) is unknown, registraion required
Invalid URI (<code>x-idp-iss</code>)	404	<code>noResource</code>	
Any other error	500	<code>internalError</code>	

neu:

description:

Sends an authorization request to the authorization service.

****Client**:**

A client shall use parameter `_x-authorize-representative_` for the "Authorize Representative" use case,

a login of a user on not owned device for representative entitlement only.

The `_x-authorize-representative_` parameter will force an authentication of the user with egK + pin only and limit the possible operations to entitlement management only.

A client shall use the returned redirect url to invoke the authenticator.

A client shall use parameter `_x-authorize-validation_` for a login of a validation identity (e.g. "Prüfkarte eGK"),

forcing the authorization service to request an authentication at the identity provider in guest mode (eGK + pin).

A client shall use the returned redirect url to invoke the authenticator.

****Provider**:**

The authorization service shall send a pushed authorization request (PAR) to the IDP (see: find more details).

The `_redirect_uri_` parameter of the PAR shall be set to a predefined value when operation parameter

`_x-redirecturi_` is not present, else the content of `_x-redirecturi_` shall be used (according to A_25717-*).

The authorize representative situation (`_x-authorize-representative_ == _true_`) shall be kept for the subsequent

`_sendAuthCodeFdV_` and device management operations.

For the `_x-authorize-representative_` and the `_x-authorize-validation_` case the PAR for the IDP shall include:

- `amr` = `urn:telematik:auth:guest:eGK`

`_x-authorize-representative_` and `_x-authorize-validation_` both should not be set to `_true_` at the same time.

The authorization service' state value and clientid used for the PAR shall occur in the URI-PAR response of the IDP.

Conditions	Status code	Error code	Remarks
-----	-----	-----	-----
Successful operation	302		
Request does not match schema	400	malformedRequest	also if both "x-authorize"-parameters are set to <code>_true_</code>
Invalid request	403	invalAuth	includes any error of Authorization Service and IDP which is not mapped to 500 internal Server error
state or clientid value mismatch	403	invalData	returned URI-PAR does not contain expected state or clientid value
unregistered redirecturi	403	invalRedir	redirecturi in <code>_x-redirecturi_</code> is not known, registration required
Invalid URI (x-idp-iss)	404	noResource	
Any other error	500	internalError	