
C_12166_Anlage

Änderungen in gemSpec_ePA_FdV:

Neue Anforderungen im Kapitel "6.1.7 ePA-FdV für Desktop-Plattformen"

A_27448 - ePA-FdV für Desktop-Plattformen - Integration eines Authenticator Moduls für Desktop-Plattformen

Das ePA-Frontend des Versicherten für Desktop Plattformen MUSS ein Authenticator Modul für Desktop-Plattformen gemäß [gemSpec_IDP_Sek#5.4] integrieren. [≤, Frontend_Vers_ePA, funkt. Eignung: Herstellererklärung]

A_27449 - ePA-FdV für Desktop-Plattformen - Authentisierung mit eGK und PIN

Das ePA-Frontend des Versicherten für Desktop Plattformen MUSS mindestens die Authentisierung am IdP mittels eGK und PIN für stationäre Endgeräte gemäß [I_Authorization_Service] unterstützen. [≤, Frontend_Vers_ePA, funkt. Eignung: Test Produkt/FA]

Hinweis: Zur Signalisierung der Anmeldung an der ePA mit eGK und PIN wird der Parameter x-authorize-egk verwendet.

A_27450 - ePA-FdV für Desktop-Plattformen - Weitere Authentifizierungsverfahren

Das ePA-Frontend des Versicherten für Desktop Plattformen KANN weitere Authentifizierungsverfahren unterstützen. [≤, Frontend_Vers_ePA, funkt. Eignung: Herstellererklärung]

Änderung im Kapitel "6.2.3.1 Authentisieren des Nutzers"

Alt:

A_26270 - ePA-Frontend des Versicherten: Nutzung von Prüfkarten und Prüfnutzeridentitäten

Für die Nutzung von Prüfkarten und Prüfnutzeridentitäten MUSS das ePA-Frontend des Versicherten die Operation send_authorization_request_fdv mit dem Parameter x-authorize_validation aufrufen [I_Authorization_Service]. [≤]

Neu:

A_26270-01 - ePA-Frontend des Versicherten: Nutzung von Prüfkarten und Prüfnutzeridentitäten

Für die Nutzung von Prüfkarten und Prüfnutzeridentitäten MUSS das ePA-Frontend des Versicherten die Operation send_authorization_request_fdv mit dem Parameter x-authorize-egk aufrufen [I_Authorization_Service]. [≤, Frontend_Vers_ePA, funkt. Eignung: Test Produkt/FA]

Änderungen in gemSpec_Aktensystem_ePAfueralle:

Änderung im Kapitel "3.17.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)"

Alt:

A_26189 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV für Validierungsaktenkonten

Falls der Eingangsparameter x-authorize-validation=True der Operation I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤, Aktensystem_ePA, funkt. Eignung: Herstellererklärung]

Neu:

A_26189-01 - Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN

Falls der Eingangsparameter x-authorize-egk=True der Operation I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤, Aktensystem_ePA, funkt. Eignung: Herstellererklärung]

Änderungen in I_Authorization_Service.yaml:

```
/epa/authz/v1/send_authorization_request_fdv:
  parameters:
    - $ref: '#/components/parameters/useragent'
  get:
    parameters:
      - $ref: '#/components/parameters/idp-iss'
      - $ref: '#/components/parameters/authorize_representative'
      - $ref: '#/components/parameters/authorize_egkvalidation'
      - $ref: '#/components/parameters/redirecturi'
    tags:
      - Authorization FdV
    operationId: sendAuthorizationRequestFdV
    summary: (sendAuthorizationRequestFdV) Send authorization request
    externalDocs:
      description: 'Request to IDP: gemSpec_IDP_FD, chapter "Anfrage von "ID_TOKEN"
        beim sektoralen Identity Provider"'
      url: https://gemspec.gematik.de/docs/gemSpec/
    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 or
      npa + pin only and limit the possible operations to entitlement management only.
      A client shall use the returned redirect url to invoke the authenticator. <br>

      A client shall use parameter _x-authorize_egkvalidation_ for a login in guest mode
      with eGK + pin of a e.g. for 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-egkvalidation_` case the PAR for the IDP shall include:

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

`_x-authorize-representative_` and `_x-authorize-egkvalidation_` 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 (e.g. <code>_x-redirecturi_</code>) is unknown, registraion required
Invalid URI (x-idp-iss)	404	noResource	
Any other error	500	internalError	

Postconditions	Remarks
<code>_authorize_representative_ kept for subsequent <code>_sendAuthCodeFdV</code> evaluation</code>	if applicable

...

components:

...

parameters:

`authorize_egkvalidation`:

name: x-authorize-egkvalidation

in: header

description: This parameter shall be absent or set to `_true_` to indicate an authorization request in guest mode with eGK + pin e.g. for validation identities.

required: false

schema:

type: boolean

enum: [true]

example: true

