

---

## C\_12470\_Anlage

---

Änderungen in `I_Authorization_Service.yaml` *sendAuthCodeFdV* description;

- *Klarstellung: "access to device management" nur im Homesystem*
- *Fehlercode: für Nutzung DeviceAttestation im HomeSystem*

**Provider:**

The provided authorization code shall be exchanged for an ID-Token with the IDP. The ID-Token shall be converted into a HSM-ID-Token with an extended validity period.

**Device verification - home system:**

If `_x-device-identifier_` and `_x-device-token_` are both submitted the device verification starts immediately after the authorization completion.

Device identifier and -token shall be verified with the registered values.

The `_x-device-identifier_` / `_x-device-token_` check shall only consider device registrations for the authorized user.

If `_x-device-identifier_` and `_x-device-token_` are both missing (i.e. not yet registered device) access of the user session shall be limited to the device management service.

**Device verification - other than home system:**

If `_x-device-attestation_` is submitted the device verification starts immediately after the authorization completion.

The authorization service shall accept a device attestation in case

- signature is valid

- "exp" expiration\_time is a timestamp 120 minutes in the future "iat".

- current time is greater or equal than "iat" and less than "exp" with 15 seconds tolerance ('iat' - 15s <= current time < 'exp' + 15s).

- claim `_actorId_` from device attestation matches kvnr of ID-Token or HSM-ID-Token.

If the device attestation is valid by signature and time, and the KVNR submitted in device attestation matches the KVNR of the authorized user the authorization service shall accept the device registration.

On success (ID-Token / HSM-ID-Token received and device binding check successful) a new user session shall be instantiated, associated to the HSM-ID-Token.

If device verification succeeds, access to all services of a health record shall be possible for the associated user session.

if `_x-authorize-representative_` is set, access to the user's health record entitlement management only shall be possible for the user session.

~~In all other (success cases) access of the user session shall be limited to the device management service.~~

The user session of a client shall be closed and all session related data shall be deleted in case operation is not successful.

The VAU user pseudonym as generated for the `vau-channel` (see: `vau` protocol) shall be returned in a successful operation response.

Conditions	Status code	Error code	Remarks
------------	-------------	------------	---------

Successful operation	200		
----------------------	-----	--	--

Request does not match schema	400	malformedRequest	
-------------------------------	-----	------------------	--

Only <code>_x-device-identifier_</code> or <code>_x-device-token_</code> provided	400	paramExpected	both parameters required or none
---	-----	---------------	----------------------------------

( <code>_x-device-identifier_</code> and/or <code>_x-device-token_</code> ) and <code>_x-device-attestation_</code> provided	400	paramExpected	use only registration of home system, another system or none (yet unregistered device)
--	-----	---------------	--

<code>_x-device-attestation_</code> provided in home system	400	paramExpected	home system shall only accept <code>_x-device-identifier_</code> and <code>_x-device-token_</code>
---	-----	---------------	--

<code>_authorize-representative_</code> is set and <code>_x-device-identifier_</code> and/or <code>_x-device-token_</code> and/or <code>_x-device-attestation_</code> provided	400	authorizeRep	<code>_x-authorize-representative_</code> from preceding <code>sendAuthorizationRequestFdV</code>
--	-----	--------------	---

Requestor role is not <code>_oid-versicherter_</code>	403	invalidOid	
---	-----	------------	--

<code>_authorizationCode_</code> not valid	403	invalidAuth	includes any error of Authorization Service and IDP which is
--	-----	-------------	--

not mapped to 500 internal Server error |  
| Wrong \_x-device-token\_ | 403 | invalidToken | if both parameters available and allowed|  
| Invalid \_x-device-attestation\_ | 403 | invalSignature ||  
| Device registration does not exist (\_x-device-identifier\_)| 404| noResource | also if device is not associated to  
requestor kvnr |  
| Device registration not confirmed (\_status\_ == \_pending\_) | 409 | statusMismatch | confirm pending device  
registration before retry |  
| Any other error | 500 | internalError | (see 'Retry interval') |