

**C_12804_Anlage - Änderungen an den Operationen zur
Anbindung von Cloud-PS**

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

2 Änderung in gemF_Personalisierung_HSM-B.....3

2.1 4.2.1 Anforderungshaushalt.....3

2.2 4.2.1.2 Nutzerauthentifizierung.....3

2.3 4.2.1.3.1 Token-Endpunkt.....3

2.4 4.2.1.3.4 Operationen zur Cloud-PS-Anbindung.....8

3 Änderung in gemILF_PS.....16

 3.1.1 8.6.2 Weitere Dokumente.....18

1 Änderungsbeschreibung

- Änderungen an den Operationen requestvKon, accessvKon, restrictvKon
 - Einführung einer eindeutigen ID für virtuelle Instanzen
 - Übergabe derClient ID im Claim "aud" des Access Token
- Neue Operation checkvKon zur Statusabfrage
- Detaillierung und Konkretisierung für Cloud-PS bzgl. Validierung von Codes und Token

2 Änderung in gemF_Personalisierung_HSM-B

2.1 4.2.1 Anforderungshaushalt

Am Ende des Absatz (vor 4.2.1.1) wir folgende AFO eingefügt

A_29680 -Umsetzung Autorisierung & Authentisierung nach OAuth2 und OIDC
Das Zugangsmodul MUSS für die Freigaben und Authentisierungen im Zuge von HSM-B-Personalisierung und Cloud-PS-Anbindung die geforderten Flows entsprechend OAuth nach [RFC6749] und OIDC nach [OpenID Connect Core] umsetzen und nur davon abweichen, sofern es per Anforderung gefordert ist.
[<=, Konnektor Highspeed, funkt. Eignung: Herstellererklärung]

2.2 4.2.1.2 Nutzerauthentifizierung

AFO A_25119 wird angepasst

Alt:

A_25119 -Authentisierungs-Endpunkt - Löschen von Authorization-Codes
Das Zugangsmodul MUSS nach A_25106 erzeugte und versendete Authorization-Codes nach 10 min aus seinem Speicher löschen, darf diese also nach Ablauf dieser Zeit nicht mehr bei der Prüfung nach A_25102* akzeptieren.[<=, TI_GW_Zugangsmodul, Sich.techn. Eignung: Produktgutachten]

Neu:

A_25119-01 -Authentisierungs-Endpunkt - Löschen von Authorization-Codes
Das Zugangsmodul MUSS nach A_25106*und A_28224*erzeugte und versendete Authorization-Codes nach deren Einlösung bzw. spätestens nach 10 min aus seinem Speicher löschen, darf diese also nur einmalig bzw. nach Ablauf dieser der genannten Zeit gar nicht mehr bei der Prüfung nach A_25102* akzeptieren.[<=, TI_GW_Zugangsmodul, Sich.techn. Eignung: Produktgutachten]

2.3 4.2.1.3.1 Token-Endpunkt

AFO A_25119-01 wird angepasst

Alt:

A_25102-01 -SMB-Service - Operation getToken
Das Zugangsmodul MUSS in seinem SMB-Service die Operation getToken als Token-Endpunkt bereitstellen.

ServiceEndpunkt	<SMB-Service-URL>/getToken
Eingangsparameter	POST parameter: <ul style="list-style-type: none">grant_type = "authorization_code" und

	<ul style="list-style-type: none"> code ist ein noch gültiger vom Authentisierungs-Endpunkt des Zugangsmodul erzeugter Authorization-Code.
Verarbeitung	<p>Das Zugangsmodul prüft auf grant_type = "authorization_code". Das Zugangsmodul prüft, ob es zu diesem Code eine Nutzerauthentifizierung gespeichert hat, die noch nicht gelöscht wurde gemäß A_25119. Das Zugangsmodul erstellt einen ID-Token wie in A_25108* (Anbieter SMC-B) oder A_26355 (Cloud-PS) beschrieben.</p>
Response	wie in A_25108*
Fehler	<ul style="list-style-type: none"> message: "Authorization-Code unbekannt oder abgelaufen", code: "SMBS_0002" message: "grant_type ungültig", Code: "SMBS_0003" message: "Interner Fehler bei der Token-Erzeugung", Code: "SMBS_0004"

52
53 **[<=, TI_GW_Zugangsmodul, funkt. Eignung: Test Produkt/FA]**

54 **Neu:**

55 **A_25102-04 -SMB-Service - Operation getToken**

56 Das Zugangsmodul MUSS in seinem SMB-Service die Operation getToken als Token-
57 Endpunkt bereitstellen.

58 **Tabelle 1 : Operation getToken des SMB-Service**

ServiceEndpoint	<SMB-Service-URL>/getToken
Eingangsparameter	<p>POST parameter:</p> <ul style="list-style-type: none"> grant_type = "authorization_code" und code ist ein noch gültiger vom Authentisierungs-Endpunkt des Zugangsmodul erzeugter Authorization-Code. redirect_uri=<URL identisch wie in A_25086*> client_id=<TSPName/Name aus TSL-Eintrag des Anbieters SMC-B>
Verarbeitung	<p>Das Zugangsmodul prüft auf grant_type = "authorization_code". Das Zugangsmodul prüft, ob es zu diesem Code eine Nutzerauthentifizierung gespeichert hat, die noch nicht gelöscht wurde gemäß A_25119. Das Zugangsmodul prüft die client_id gemäß A_25109*. Das Zugangsmodul erstellt einen ID-Token wie in A_25108* (Anbieter SMC-B) oder bzw. einen ID-Token und Access-Token wie in A_26355* (Cloud-PS) beschrieben.</p>
Response	wie in A_25108* bzw. A_26355*

Fehler	<ul style="list-style-type: none">• message: "Authorization-Code unbekannt oder abgelaufen", code: "SMBS_0002"• message: "grant_type ungültig", Code: "SMBS_0003"• message: "Interner Fehler bei der Token-Erzeugung", Code: "SMBS_0004"
--------	--

[<=, TI_GW_Zugangsmodule, funkt. Eignung: Test Produkt/FA]

AFO A_26355 wird angepasst

Alt:

A_26355 -Cloud-PS-Anbindung: Token-Endpunkt - Response im Erfolgsfall (Cloud-PS)

Das Zugangsmodule MUSS genau nur wenn die Prüfungen nach A_25102* erfolgreich waren:

den folgenden signierten ID-Token anhand der dem Authorization-Code zugeordneten Daten erzeugen:

```
{ "iss": "<URL entsprechend TSL-Eintrag nach A_25104>",  
  "sub": "<GatewayUserID authentifizierter Nutzer>",  
  "aud": "<Cloud-PS Name (client_id)>",  
  "nonce": "<nonce aus Anfrage>",  
  "exp": "<Ausstellungsdatum iat + 300 Sekunden>",  
  "iat": "<aktuelle Zeit als Sekunden seit 1970-01-01T00:00:00Z in UTC>" }
```

den folgenden Access Token, wobei nur die angeforderten scope-Einträge zurückgemeldet werden:

```
{ "sub": "<GatewayUserID authentifizierter Nutzer>",  
  "iat": "aktuelle Zeit als Sekunden seit 1970-01-01T00:00:00Z in UTC",  
  "exp": "<Ausstellungsdatum iat + 300 Sekunden>",  
  "scope": "read:vKon use:vKon configure:vKon" }
```

Token Signatur:

JSON Web Signature (JWS) nach RFC7515 mit ECDSA mit P-256 und SHA-256 und entsprechendem Header:

```
{ "typ": "JWT",  
  "alg": "ES256" }
```

diesen im weiteren als JWS in Compact Serialization verwenden:

BASE64(Header).BASE64(ID-Token).BASE64(Signature)

und dem Cloud-PS wie folgt antworten:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "access_token": "<Acces-Token>",
  "token_type": "bearer",
  "expires_in": 300,
  "id_token": "<ID-Token in JWS Compact Serialization>",
}
```

[<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

Neu:

A_26355-01 -Cloud-PS-Anbindung: Token-Endpunkt - Response im Erfolgsfall (Cloud-PS)

Das Zugangsmodule MUSS genau nur wenn die Prüfungen nach A_25102* erfolgreich waren:

den folgenden signierten ID-Token anhand der dem Authorization-Code zugeordneten Daten erzeugen:

```
{ "iss": "<URL entsprechend TSL-Eintrag nach A_25104>",
  "sub": "<GatewayUserID authentifizierter Nutzer>",
  "aud": "<Cloud-PS Name (client_id)>",
  "nonce": "<nonce aus Anfrage>",
  "exp": "<Ausstellungsdatum iat + 300 Sekunden>",
  "iat": "<aktuelle Zeit als Sekunden seit 1970-01-01T00:00:00Z in UTC>"
}
```

den folgenden signierten Access-Token, wobei nur die angeforderten scope-Einträge zurückgemeldet werden:

```
{ "iss": "<URL entsprechend TSL-Eintrag nach A_25104>",
  "sub": "<GatewayUserID authentifizierter Nutzer>",
  "aud": "<Cloud-PS Name (client_id)>",
  "iat": "aktuelle Zeit als Sekunden seit 1970-01-01T00:00:00Z in UTC",
  "exp": "<Ausstellungsdatum iat + 300 Sekunden>",
  "scope": "read:vKon use:vKon configure:vKon" }
```

Token Signatur:

JSON Web Signature (JWS) nach [RFC7515] mit ECDSA mit P-256 und SHA-256 und entsprechendem Header:

```
{ "typ": "JWT",
  "alg": "ES256",
  "kid": "<Referenz zum öffentlichen Signaturschlüssel unter jwks_uri>"
}
(die Angabe der kid ist verpflichtend, wenn mehrere Schlüssel im jwks veröffentlicht werden)
```

diesen im weiteren als JWS in Compact Serialization verwenden:

153

155 BASE64(Header).BASE64(ID-Token).BASE64(Signature)

156

157 **und dem Cloud-PS wie folgt antworten:**

159 HTTP/1.1 200 OK

160 Content-Type: application/json;charset=UTF-8

161 Cache-Control: no-store

162 Pragma: no-cache

163

164 {

165 "access_token": "<Access-Token>",

166 "token_type": "bearer",

167 "expires_in": 300,

168 "id_token": <ID-Token in JWS Compact Serialization>,

169 }

170 [<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test
171 Produkt/FA]

172

173

2.4 4.2.1.3.4 Operationen zur Cloud-PS-Anbindung

AFO A_26356-01 wird angepasst

Alt:

A_26356-01 -Cloud-PS-Anbindung: Operation requestvKon

Das Zugangsmodul MUSS am SMB-Service die Operation requestvKon anbieten.

Service Endpunkt	<SMB-Service-URL>/requestvKon
Eingangsparameter	GET Authorization: Bearer <ID-Token> <ACCESS_TOKEN>
Verarbeitung	<ol style="list-style-type: none">1. Prüfe die Signatur von ID-Token und Access-Token2. Extrahiere GatewayUserID aus access und ID Token. prüfe auf Identität3. extrahiere client_id aus sub und prüfe ob konfiguriertes Cloud-PS4. Prüfe access_token auf scope read:vKon5. Rückmeldung an den Aufrufer
Rückgabe	Liste der HSK-Instanzen { vkon: [{ name : "Name der HSK-Instanz" ; ip : "IP-Adresse der HSK-Instanz" }] }
Fehlermeldung	zu (1): code: "SMBS_10010", message: "Tokensignature ungültig" zu (2): code: "SMBS_10011", message: "UserID in Token nicht gleich" zu (3): code: "SMBS_10012", message: "Cloud-PS unbekannt" zu (4): code: "SMBS_10013", message: "Operation nicht autorisiert" zu (5): Wenn keine HSK-Instanz ermittelt wird, ist das kein Fehler, sondern meldet eine leere Liste zurück: {vkon: [] } sonst: code: "SMBS_10015", message: "Fehler in der Operation"

s[<=, TI_GW_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

Neu:

A_26356-02 -Cloud-PS-Anbindung: Operation requestvKon

Das Zugangsmodul MUSS am SMB-Service die Operation requestvKon anbieten.

185

Tabelle 2 : Operation requestvKon des SMB-Service

Service Endpunkt	<SMB-Service-URL>/requestvKon
Eingangsparameter	GET Authorization: Bearer <ID-Token> <Access-Token>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von ID-Token und Access-Token 2. Prüfe dass Systemzeit <= exp Extrahiere GatewayUserID aus access und ID-Token. prüfe auf Identität 3. Extrahiere client_id aus aud sub und prüfe ob konfiguriertes Cloud-PS 4. Prüfe Access-Token auf scope read:vKon 5. Rückmeldung an den Aufrufer
Rückgabe	Liste der virtuellen KonnektorHSK-Instanzen <pre>{ "vkon": [{ "id" : "ID der vInstanz", name : "Name der HSK- vInstanz", ip : "IP-Adresse der HSK- vInstanz" }] }</pre>
Fehlermeldung	zu (1): code: "SMBS_10010", message: "Tokensignature ungültig" zu (2): code: "SMBS_10011", message: "Access Token abgelaufenUserID in Token nicht gleich" zu (2): code: "SMBS_10012", message: "Cloud-PS unbekannt" zu (3): code: "SMBS_10013", message: "Operation nicht autorisiert" zu (5): Wenn keine HSK-Instanz ermittelt wird, ist das kein Fehler, sondern meldet eine leere Liste zurück: {vkon: [] } sonst: code: "SMBS_10015", message: "Fehler in der Operation"

186

187

188

189

[<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

190

191

[AFO A_28225-01 wird angepasst](#)

192

Alt:

193

A_28225-01 -Cloud-PS-Anbindung: Operation accessvKon

194

Das Zugangsmodul MUSS am SMB-Service die Operation accessvKon anbieten.

Service Endpunkt	<SMB-Service-URL>/accessvKon
Eingangsparameter	<p>POST</p> <pre>{ vkon : [{ name : "Name der HSK-Instanz" ; ip: "IP-Adresse der HSK-Instanz" }] }</pre>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von ID_Token und Access_Token 2. Extrahiere GatewayUserID aus access und ID Token. prüfe auf Identität 3. extrahiere client_id aus sub und prüfe ob konfiguriertes Cloud-PS 4. Prüfe ob die übergebene(n) HSK-Instanz-IP(s) der GatewayUserID gehört. 5. Wenn der Scope des access_tokens use:vKon enthält, schalte Firewall für Client_id zur den SOAP, LDAP, CETP und SICCT Interfaces des übergebenen HSK-Instanz-IP frei 6. Wenn der Scope des access_tokens configure:vKon enthält, schalte Firewall für Client_id und für 60 min zum Admin Interfaces des übergebenen HSK-Instanz-IP frei
Rückgabe	code: "SMBS_1001", message: "Access granted"
Fehlermeldung	<p>zu (1): code: "SMBS_10010", message: "Tokensignature ungültig"</p> <p>zu (2): code: "SMBS_10011", message: "UserID in Token nicht gleich"</p> <p>zu (3): code: "SMBS_10012", message: "Cloud-PS unbekannt"</p> <p>zu (4): code: "SMBS_10014", message: "vKon nicht autorisiert"</p> <p>wenn der Scope weder use:vKon noch configure:vKon enthält: code: "SMBS_10013", message: "Operation nicht autorisiert"</p> <p>sonst: code: "SMBS_10015", message: "Fehler in der Operation"</p>

196
197 **[<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test**
198 **Produkt/FA]**

199 **Neu:**

200 **A_28225-02 -Cloud-PS-Anbindung: Operation accessvKon**

201 Das Zugangsmodul MUSS am SMB-Service die Operation accessvKon anbieten.

Tabelle 3 : Operation accessvKon des SMB-Service

Service Endpunkt	<SMB-Service-URL>/accessvKon
Eingangsparameter	<p>POST</p> <p><ID_TOKEN> <Access_Token></p> <pre>{ vkon : [{ "id" : "vInstanz-ID" name : "Name der HSK Instanz"; ip: "IP-Adresse der HSK Instanz" }] }</pre>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von ID-Token und Access_Token 2. Prüfe dass Systemzeit <= exp Extrahiere GatewayUserID aus access und ID-Token. prüfe auf Identität 3. Extrahiere client_id aus audsub und prüfe ob konfiguriertes Cloud-PS 4. Prüfe ob die übergebenen HSK- vInstanz-IDs IP(s) der GatewayUserID gehören 5. Wenn der Scope des Access_Token use:vKon enthält, schalte Firewall für Client_id zu den SOAP, LDAP, CETP und SICCT Interfaces der übergebenen HSK- vInstanz-IDs IP frei 6. Wenn der Scope des Access_Token configure:vKon enthält, schalte Firewall für Client_id und für 60 min zum Admin Interfaces der übergebenen HSK-vInstanz-IDs IP frei
Rückgabe	<p>Wenn Vorgang erfolgreich abgeschlossen code: "SMBS_1001", message: "Access granted"</p> <p>Wenn Vorgang noch in Bearbeitung code: "SMBS_1003", message: "Access pending"</p>
Fehlermeldung	<p>zu (1): code: "SMBS_10010", message: "Tokensignature ungültig"</p> <p>zu (2): code: "SMBS_10011", "Access Token abgelaufen UserID in Token nicht gleich"</p> <p>zu (3): code: "SMBS_10012", message: "Cloud-PS unbekannt"</p> <p>zu (4): code: "SMBS_10014", message: "vKon nicht autorisiert"</p> <p>wenn der Scope weder use:vKon noch configure:vKon enthält: code: "SMBS_10013", message: "Operation nicht autorisiert"</p>

	sonst: code: "SMBS_10015", message: "Fehler in der Operation"
--	---

203
204 [\leq , TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test
205 Produkt/FA]

206
207 [AFO A_28226-01 wird angepasst](#)

208 **Alt:**

209 **A_28226-01 -Cloud-PS-Anbindung: Operation restrictvKon**

210 Das Zugangsmodule MUSS am SMB-Service die Operation restrictvKon anbieten.

Service Endpunkt	<SMB-Service-URL>/restrictvKon
Eingangsparameter	POST <pre>{ vkon : [{ name : "Name der HSK-Instanz" ; ip: "IP-Adresse der HSK-Instanz" }] }</pre>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von ID_Token und Access_Token 2. Extrahiere GatewayUserID aus access und ID Token. prüfe auf Identität 3. extrahiere client_id aus sub und prüfe ob konfiguriertes Cloud-PS 4. Prüfe ob die übergebene(n) HSK-Instanz-IP(s) der GatewayUserID gehört. 5. Sperre die Firewall für Client_id zur übergebenen HSK-Instanz-IP. Wenn keine HSK-Instanz Liste übergeben wurde, sperre alle HSK-Instanzen dieser Client_Id
Rückgabe	code: "SMBS_1002", message: "Access withdrawn"
Fehlermeldung	zu (1): code: "SMBS_10010", message: "Tokensignature ungültig" zu (2): code: "SMBS_10011", message: "UserID in Token nicht gleich" zu (3): code: "SMBS_10012", message: "Cloud-PS unbekannt" zu (4): code: "SMBS_10014", message: "vKon nicht autorisiert" sonst: code: "SMBS_10015", message: "Fehler in der

	Operation"
--	------------

[<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test
Produkt/FA]

Neu:

A_28226-02 -Cloud-PS-Anbindung: Operation restrictvKon

Das Zugangsmodul MUSS am SMB-Service die Operation restrictvKon anbieten.

Tabelle 4 : Operation restrictvKon des SMB-Service

Service Endpunkt	<SMB-Service-URL>/restrictvKon
Eingangsparameter	<pre> POST <ID_TOKEN> <Access_Token> { "vkon" : [{ "id" : "vInstanz-ID" name : "Name der HSK Instanz"; ip: "IP-Adresse der HSK Instanz" }] }</pre>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von ID-Token und Access-Token 2. Prüfe dass Systemzeit <= exp Extrahiere GatewayUserID aus access und ID-Token. prüfe auf Identität 3. Extrahiere client_id aus aud sub und prüfe ob konfiguriertes Cloud-PS 4. Prüfe Access-Token auf scope *:vKon 5. Prüfe ob die übergebenen vInstanz-ID's HSK Instanz-IP(s) der GatewayUserID gehören 6. Sperre die Firewall für Client_id zu den übergebenen vInstanz-ID's HSK Instanz-IP. Wenn keine HSK-vInstanz- Liste übergeben wurde, sperre alle HSK-vInstanzen dieser Client_Id
Rückgabe	<p>Wenn Vorgang erfolgreich abgeschlossen code: "SMBS_1002", message: "Access withdrawn"</p> <p>Wenn Vorgang noch in Bearbeitung code: "SMBS_1004", message: "Restriction pending"</p>
Fehlermeldung	<p>zu (1): code: "SMBS_10010", message: "Tokensignature ungültig"</p> <p>zu (2): code: "SMBS_10011", message: "Access Token abgelaufen UserID in Token nicht gleich"</p> <p>zu (3): code: "SMBS_10012", message: "Cloud-PS</p>

	unbekannt" zu (4): code: "SMBS_10013", message: "Operation nicht autorisiert" zu (45): code: "SMBS_10014", message: "vKon nicht autorisiert" sonst: code: "SMBS_10015", message: "Fehler in der Operation"
--	---

219
220 **[<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test**
221 **Produkt/FA]**

222 [Neue Anforderung](#)

223 **A_29683 -Cloud-PS-Anbindung: Operation checkvKon**

224 Das Zugangsmodul MUSS am SMB-Service die Operation checkvKon anbieten.

225 **Tabelle 5 : Operation checkvKon der SMB Service**

Service Endpunkt	<SMB-Service-URL>/checkvKon
Eingangsparameter	POST Authorization: Bearer <Access_Token> <pre>{ "vkon" : [{ "id" : "vInstanz-ID" }] }</pre>
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe die Signatur von Access_Token 2. Prüfe dass Systemzeit <= exp + 3600 Sekunden 3. Extrahiere client_id aus aud und prüfe ob konfiguriertes Cloud-PS 4. Prüfe Access_Token auf scope *:vKon 5. Prüfe ob die übergebenen vInstanz-IDs der GatewayUserID gehören
Rückgabe	<pre>{ "vkon" : [{ "id" : "vInstanz-ID", "grantedScopes" : ["use:vKon", "configure:vKon"] }], "retrievedAt" : "datetime" }</pre> <p>grantedScopes: aktueller Freischaltungsstatus der vInstanz retrievedAt: Zeitpunkt der Statusbereitstellung</p>

Fehlermeldung	zu (1): code: "SMBS_10010", message: "Tokensignatur ungültig" zu (2): code: "SMBS_10011", message: "Access Token abgelaufen" zu (3): code: "SMBS_10012", message: "Cloud-PS unbekannt" zu (4): code: "SMBS_10013", message: "Operation nicht autorisiert" zu (5): code: "SMBS_10014", message: "vKon nicht autorisiert" sonst: code: "SMBS_10015", message: "Fehler in der Operation"
---------------	--

【<=, TI_GW_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test
Produkt/FA】

3 Änderung in gemILF_PS

Nach dem Einleitungsabsatz wird folgender Text eingefügt:

Im Folgenden werden virtuelle Konnektor-Instanzen die in den HSKs laufen als vInstanzen bezeichnet.

Neue AFO unter dem neu eingefügten Text / über A_26357

A_29679 -Umsetzung Autorisierung & Authentisierung nach OAuth2 und OIDC

Das Cloud-PS MUSS für die Freigabe des TI-GW-Nutzers zum Zugriff des Cloud-PS auf dessen vInstanz die geforderten Flows entsprechend OAuth nach [RFC6749] und OIDC nach [OpenID Connect Core] umsetzen und nur davon abweichen, sofern es im ILF per Anforderung gefordert ist.

[<=, ,]

Die AFO A_28222 wird wie folgt angepasst und **von gemF_Personalisierung_HSM-B nach gemILF_PS verschoben** und dort unter A_29679 eingefügt.

Alt:

A_28222 -Redirect zur Authentifizierung am TI-Gateway (Cloud-PS)

Das Cloud-PS MUSS einen Auth-Request nach RFC 6749 mittels Redirect zum Cloud-PS Authentisierungs-Endpunkt des gewählten Anbieters TI-Gateway senden. Der Auth-Request muss folgendermaßen parametrierung werden:

HTTP/1.1 302 Found

Location: <URL Authentisierungs-Endpunkt entsprechend A_25116*>?

response_type=code

&scope=openid read:vKon use:vKon configure:vKon

&client_id=<Cloud-PS Name wie zwischen Cloud-PS und TI-GW vereinbart>

&state=<Random-String>

&nonce=<individuelle 10 Minuten gültige Zufallszahl>

&redirect_uri=<Endpunkt zur Verarbeitung von Auth-Codes>

Das Cloud-PS muss für die späteren Auswertungen die Kombination von Anbieter TI-Gateway, state und nonce persistieren, wobei das Cloud-PS durchsetzen MUSS, dass jede nonce nur einmalig verwendet und nach 10 Minuten gelöscht wird.

Das Cloud-PS MUSS den scope read:vKon senden, um die HSK-Instanz des Nutzers abzurufen.

Das Cloud-PS MUSS den scope use:vKon senden, um eine HSK-Instanz zur Nutzung freizuschalten.

Das Cloud-PS MUSS den scope configure:vKon senden, um das Admin-Interface der HSK-Instanz freizuschalten.

[<=, ,]

Neu:

A_28222-01 -Redirect zur Authentifizierung am TI-Gateway (Cloud-PS)

Das Cloud-PS MUSS einen Auth-Request nach [RFC6749] mittels Redirect zum Cloud-PS Authentisierungs-Endpunkt des gewählten Anbieters TI-Gateway senden. Der Auth-Request muss folgendermaßen parametrierung werden:

HTTP/1.1 302 Found

Location: <URL Authentisierungs-Endpunkt entsprechend A_25116*>?

response_type=code


```
&scope=openid read:vKon use:vKon configure:vKon
&client_id=<Cloud-PS Name wie zwischen Cloud-PS und TI-GW vereinbart>
&state=<individuelle 10 Minuten gültige Zufallszahl != nonce>
&nonce=<individuelle 10 Minuten gültige Zufallszahl != state>
&redirect_uri=<Endpunkt zur Verarbeitung von Authorization Codes>
```

Das Cloud-PS muss für die späteren Auswertungen die Kombination von Cloud-PS-Nutzer-Session, Anbieter TI-Gateway, state und nonce persistieren, wobei das Cloud-PS durchsetzen MUSS, dass jede nonce und state nur einmalig verwendet und nach 10 Minuten gelöscht wird.

Das Cloud-PS MUSS den scope read:vKon senden, um die vInstanzen des Nutzers abzurufen.

Das Cloud-PS MUSS den scope use:vKon senden, um vInstanzen zur Nutzung freizuschalten.

Das Cloud-PS MUSS den scope configure:vKon senden, um das Admin-Interface von vInstanzen freizuschalten.

[<=, ,]

[Hinweis unter A_28222-01](#)

Hinweis: Um mit einem Access Token später mehrere Aktionen für einen Nutzer durchführen zu können (bspw. Informationen zur vInstanz abrufen und vom Nutzer gewünschte Freischaltungen am TI-Gateway durchführen), müssen alle benötigten Scopes in einem Auth-Request angegeben werden. Werden separate Auth-Requests verwendet, muss der Nutzer mehrfach die Authentifizierung beim TI-Gateway Anbieter durchlaufen.

[Neue AFO unter A_28222-01](#)

A_29681 -Verarbeitung Authorization Code durch Cloud-PS

Das Cloud-PS MUSS unter der redirect_uri (vgl. A_28222*) empfangene Requests hinsichtlich des Parameters state prüfen, ob dieser für die aktuelle PS-Nutzer-Session valide ist und nur im Erfolgsfall:

- eine mTLS-Verbindung zum mit state verknüpften TI-Gateway Anbieter aufbauen,
- dabei sein beim TI-Gateway Anbieter konfiguriertes TLS-Client-Zertifikat verwenden,
- das TLS-Server-Zertifikat des TI-Gateway Anbieters prüfen, dass es dem für diesen Anbieter hinterlegten Zertifikat entspricht,
- über die erfolgreich aufgebaute mTLS-Verbindung einen Token-Request senden (getToken, vgl. A_25102*) mit
 - grant_type=authorization_code
 - code=<Authorization Code>
 - redirect_uri=<URL identisch wie in A_28222*>
 - client_id=<Cloud-PS Name>
- aus der Token-Response ID-Token und Access-Token extrahieren und entsprechend A_29682* auswerten.

[<=, ,]

[Neue AFO unter A_29681](#)

A_29682 -Auswertung ID-Token und Access-Token durch Cloud-PS

Das Cloud-PS MUSS einen mittels getToken vom TI-Gateway empfangenen ID-Token und Access-Token wie folgt auswerten:

- Prüfen, dass im ID-Token im Feldiss der Anbieter TI-Gateway genannt ist, von dem entsprechend A_29681* die Token bezogen wurden.
- Laden des C.FD.OSIG Zertifikat dieses TI-Gateway Anbieters (vgl. A_25116*), wenn mehrere Zertifikate gefunden werden, wird der Parameterkid aus dem Token für die Auswahl ausgewertet.
- Prüfen der Signatur beider Token gegen das ermittelte C.FD.OSIG.
- Anhand des Zeitstempels im Feldiat jeweils prüfen, dass die Token nicht älter als 5 Minuten sind.
- Prüfen, dass die Feldersub in beiden Token identisch sind, also den selben TI-Gateway-Nutzer betreffen.
- Dienonce im ID-Token auf Gültigkeit prüfen und dass diese zur aktuellen PS-Nutzer-Session passt, aus der auch Authorization Code empfangen wurde (vgl. A_29681).
- Ausschließlich wenn alle vorangegangenen Prüfungen erfolgreich durchlaufen wurden: Das mit dem ID-Token zusammen erhaltene Access-Token dem PS-Nutzer-Account dieser PS-Nutzer-Session und somit der ursprünglichen Authentisierungsanfrage (A_28222*) für die weitere Nutzung zuordnen.

[<=, ,]

[Ergänzung bei Referenzierte Dokumente](#)

3.1.1 8.6.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[OpenID Connect Core]	OpenID Connect Core 1.0 (incorporating errata set 2, 15, December 2023) https://openid.net/specs/openid-connect-core-1_0.html
[RFC6749]	The OAuth 2.0 Authorization Framework (October 2012) https://datatracker.ietf.org/doc/html/rfc6749