
C_11948_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Änderung in gemF_TI-Gateway.....	5
3 Änderung in gemF_PersonalisierungHSM-B.....	8
4 Änderung in gemILF_PS.....	15

1 Änderungsbeschreibung

Vom Gesetz (§393 SGB V) sind Rahmenbedingungen für die Verarbeitung von Medizinischen Daten in der Cloud festgelegt. Mit der aktuellen Spezifikationslage ist eine skalierbare und performante Nutzung des TI-Gateway nicht möglich. Mit diesem Change werden Rahmenbedingungen und Mechanismen definiert, um eine effiziente Anbindung Cloudbasierter Clientsysteme an ein TI-Gateway zu ermöglichen.

- Für cloudbasierte Clientsysteme im Sinne von § 393 SGB V wird die Bezeichnung Cloud-PS eingeführt. Damit sollen auch Clientsysteme umfasst werden, die nicht im engeren Sinne Primärsysteme sind.
- Das Anbindungsmodul für Cloud-PS ist ein optionales Modul des TI-Gateway Zugangsmoduls
- Nach der bestehenden Spezifikation gehört jede VPN-Verbindung genau einem TI-Gateway-Nutzer und bestimmt, welche HSK-Instanzen erreicht werden können. Bei der Cloud-PS Anbindung ist die Netzanbindung zwischen Cloud-PS und TI-Gateway vom TI-Gateway-Nutzer unabhängig. Wie schon für angeschlossene DVO wird durch den TI-Gateway-Nutzer im Zugangsmodul festgelegt, welche HSK-Instanzen ein Cloud-PS erreichen kann. Alle Zugriffswege können dabei parallel bestehen (Nutzer-VPN, freigegebener DVO, freigegebenes Cloud-PS).
- Es wird spezifiziert welche Funktionen das TI-Gateway übernimmt und welche über den Implementierungsleitfaden an das Primärsystem delegiert werden.
- Der Zugriff auf die HSK-Instanz eines Nutzers ist nur nach Autorisierung durch den Nutzer mit seinen Credentials des TI-Gateways möglich. Hierfür wird ein interoperabler Mechanismus spezifiziert durch Erweiterung des SMB-Service.
- Cloud-PS und TI-Gateway müssen eine vertragliche Verbindung eingehen. Die Anbindungen sind nicht exklusiv, so dass ein Cloud-PS mehrere TI-Gateways anbinden kann aber auch ein TI-Gateway mehrere Cloud-PS. Nach der vertraglichen Vereinbarung stellen Cloud-PS und TI-Gateway die technische Verbindung her z.B. durch den Austausch von VPN-Adressen und Credentials
- Der Nutzer eines Cloud-PS kann nur die TI-Gateways nutzen, die an dieses Cloud-PS angebunden wurden. Ggf. wählt er im Cloud-PS sein TI-Gateway aus der Liste der angebundenen TI-Gateways aus.
- Die IP-Adressen der HSK-Instanzen seiner Mandanten muss das Cloud-PS nach Autorisierung durch den TI-Gateway-Nutzer direkt vom TI-Gateway mit dem dafür spezifizierten Service beziehen. Für die Admin-Credentials der HSK-Instanzen wurde kein neuer Prozess definiert.
- Die Zugangsberechtigung des Cloud-PS auf eine HSK-Instanz kann über zwei Wege Entzogen werden. Vom Cloud-PS über den dafür definierten Service oder vom TI-Gateway-Nutzer über das Nutzerportal
- Durch den spezifizierten OIDC-Mechanismus kann das Erstellen einer TI-Verbindung in die Workflows des Cloud-PS integriert werden.

Begriffe:

HSK-Instanz : virtueller Konnektor innerhalb eines HSK abgekürzt vKon

TI-Gateway-Nutzer : Kunde des TI-Gateways, der sich mit zwei-Faktor Authentifizierung am Userportal des TI-Gateways anmeldet und ein oder mehrere HSK-Instanzen verwaltet. Das kann ein Leistungserbringer sein, aber auch eine übergeordnete Organisation für mehrere Leistungserbringerinstitutionen.

2 Änderung in gemF_TI-Gateway

Anpassungen in 5.3 Routing und Firewall

A_23246 wird abgelöst, da durch nachfolgende AFOs abgedeckt.

A_23370 wird abgelöst durch

A_23370-01 -Verbindungen zum Administrationsinterface einer HSK-Instanz

Das TI-GW-Zugangsmodule MUSS sicherstellen, dass Verbindungen zum Administrationsinterface einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution und nach Berechtigung durch den Nutzer aus dem Netz eines angeschlossenen DVOs oder Cloud PS möglich sind.

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

A_23394-01 wird abgelöst durch

A_23394-02 -Verbindungen zu fachlichen Interfaces einer HSK-Instanz

Das TI-GW-Zugangsmodule MUSS sicherstellen, dass Verbindungen zu den fachlichen Interfaces einer HSK-Instanz SOAP, LDAP, CETP und SICCT nur aus dem Netz der zugeordneten LE-Institution und zu den fachlichen Interfaces SOAP, LDAP und CETP (SICCT explizit nicht) nach Autorisierung durch den Nutzer aus dem Netz eines angeschlossenen Cloud-PS möglich sind. Verbindungen zu fachlichen Interfaces aus dem Netz eines angeschlossenen DVO MÜSSEN unterbunden werden.

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

A_28335 -Verbindungen zu offenen Fachdiensten und WANDA

Das TI-GW-Zugangsmodule MUSS Verbindungen zu offenen Fachdiensten und WANDA aus angeschlossenen LE-Netzen zulassen, wenn auf einem HSK des Nutzers eine SM-B freigeschaltet ist. Wenn die Verbindungen zum HSK geroutet werden, kann die Prüfung der SMC-B Freischaltung vom HSK vorgenommen werden.

Das TI-GW-Zugangsmodule MUSS Verbindungen zu offenen Fachdiensten und WANDA von angeschlossenen Cloud-PS zulassen. [<=,TI_GW_Zugangsmodule,Sich.techn. Eignung: Produktgutachten]

Es wird Kapitel 5.3.1 neu aufgenommen

5.3.1 Anbindung von Cloud-PS

Wenn statt einer Nutzerumgebung ein Clientsystem nach den Maßgaben von SGBV § 393 (Cloud-PS) an das TI-Gateway angebunden ist, kann dieses auch unabhängig vom Kontext eines TI-Gateway-Nutzers mit dem Zugangsmodule verbunden werden. Es gelten dann nicht die Zugangsmechanismen von VPN-Anbindungen, sondern eigene Mechanismen, wie nachfolgend beschrieben. Eine HSK-Instanz kann dabei sowohl für den Zugriff eines Cloud-PS als auch für den Zugriff über VPN genutzt werden. Die technischen Rahmenbedingungen für die Anbindung zwischen Cloud-PS und TI-Gateway sind Analog zu den VPN-Anbindungen der TI-Gateway-Nutzer.

A_28377 -Modul Cloud-PS-Anbindung

Das Zugangsmodule KANN das Feature Cloud-PS-Anbindung umsetzen.

[<=,TI_GW_Zugangsmodule,funkt. Eignung: Herstellererklärung]

A_26391 -Cloud-PS-Anbindung: Zugriff durch Cloud-PS nur nach Freigabe durch TI-Gateway-Nutzer

Das Zugangsmodul MUSS dem TI-Gateway-Nutzer ermöglichen, den Zugriff eines Cloud-PS auf seinen HSK-Instanz freizugeben und wieder zu sperren.

Das Zugangsmodul MUSS durchsetzen, dass genau nur für die Cloud-PS, für die der TI-Gateway-Nutzer eine Freigabe erteilt hat, die HSK-Instanzen dieses Nutzers erreichbar sind. Initial ist nach der Registrierung / Anbindung eines Cloud-PS somit für diesen keine HSK-Instanz erreichbar. Die Freigabe MUSS der TI-Gateway-Nutzer direkt im Portal des TI-Gateways erteilen können und mittelbar über den SMB-Service.

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

A_28221 -Cloud-PS-Anbindung: Zugriff auf Admin-Interface nur nach Freigabe durch TI-Gateway-Nutzer

Das Zugangsmodul (zentrale Komponente) MUSS durchsetzen, dass der Verbindungsaufbau aus dem Netz eines Cloud-PS zu dem Admin-Interface eines HSK-Instanz nur nach expliziter Freigabe durch den Nutzer zugelassen wird und auf eine Sitzung begrenzt ist, die eine maximale Laufzeit von 1h haben darf.

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

Um Missbrauch durch Innentäter aus dem Cloud-PS zu entgegenzuwirken, ist der Zugriff auf eine Stunde begrenzt. Wenn das Cloud-PS darüber hinaus Konfigurationen vornehmen möchte, kann dieses jederzeit erneut durch den TI-Gateway-Nutzer autorisiert werden. Die direkte Autorisierung des Cloud-PS soll es ermöglichen, für das Onboarding notwendige Konfigurationsaufgaben im Cloud-PS umzusetzen und so eine durchgehende Nutzererfahrung möglich zu machen. Alternativ steht für die betriebliche Betreuung das Feature "Angeschlossene DVO-Netze" zur Verfügung, welches eine dauerhafte Erreichbarkeit der HSK-Admin-Interfaces bietet.

Nachfolgende Anforderungen an die Anbieter TI-Gateway ergänzen passende Anforderungen an Cloud-PS.

A_26353 -Cloud-PS-Anbindung: TI-Zugang nur mit SMC-B / HSM-B

Der Anbieter des TI-Gateway MUSS angeschlossene Cloud-PS vertraglich verpflichten, seinen Nutzern nur Zugang zur TI zu ermöglichen, wenn der jeweilige Nutzer seine Berechtigung durch Freischaltung einer SMC-B oder Aktivierung eines HSM-B nachgewiesen hat.[<=,Anb_TI_Gateway,funkt. Eignung: Anbietererklärung]

A_26354 -Cloud-PS-Anbindung: Missbrauchserkennung bei Cloud-PS

Der Anbieter des TI-Gateway MUSS angeschlossene Cloud-PS vertraglich verpflichten, eine Mechanismen zur Erkennung und Unterbindung missbräuchlichen Nutzung der TI in ihren Systemen zu implementieren.

[<=,Anb_TI_Gateway,funkt. Eignung: Anbietererklärung]

A_26442 -Cloud-PS-Anbindung: Cloud-PS in den Betriebsdaten

Der Anbieter TI-Gateway / das Zugangsmodul MÜSSEN in den Bestandsdaten des Zugangsmoduls folgendes melden:

- die Anzahl der angeschlossenen Cloud-PS und
- die Anzahl der HSK-Instanzen, auf die mindestens ein Cloud-PS zugreifen kann.

[<=,TI_GW_Zugangsmodul, Anb_TI_Gateway,organ./betriebl. Eignung: Prozessprüfung, funkt. Eignung: Test Produkt/FA]

Betriebsdaten werden vom Anbieter Typ I für alle Anbieter gesendet, die dieses TI-Gateway nutzen.

ToDo: Umsetzung in gemSpec_Perf

A_26438 -Cloud-PS-Anbindung: Nur Anbindung von Cloud-PS nach SGB V §393

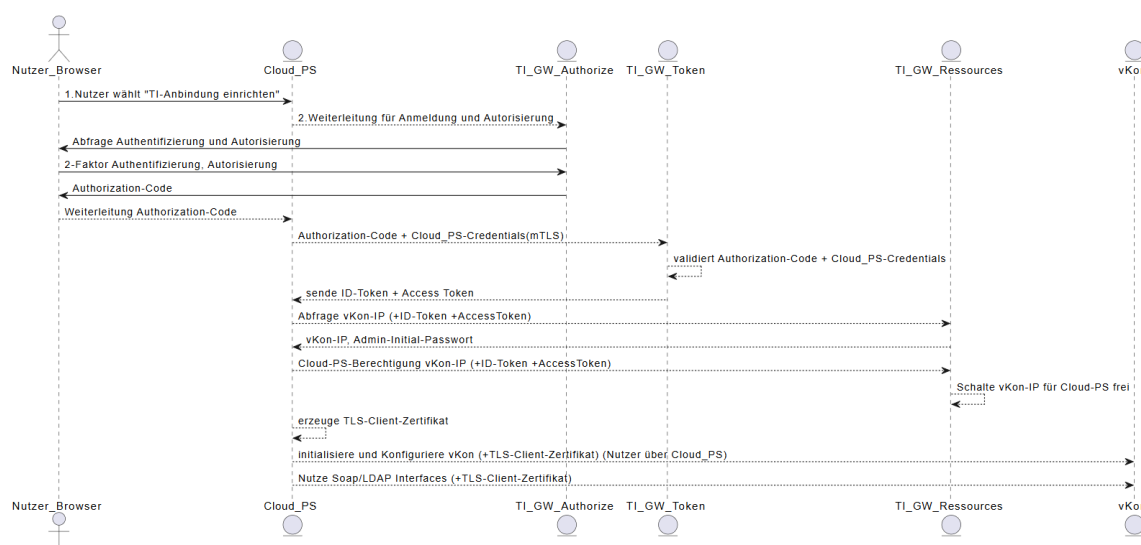
Der Anbieter TI-Gateway MUSS sicherstellen, dass er ausschließlich solche Cloud-PS anschließt, die unter die Regelung von §393 des SGB V fallen und sich sowohl vor Anschluss als auch jährlich davon überzeugen, dass das Cloud-PS die Vorgaben des §393 SGB V umsetzt.【<=,Anb_TI_Gateway,funkt. Eignung: Anbietererklärung】

3 Änderung in gemF Personalisierung HSM-B

neues Kapitel

3.4 OAuth für Cloud-PS Anbindung

Der SMB-Service des TI-Gateway-Zugangsmoduls wird erweitert, um die Prozesse der Cloud PS Anbindung zu unterstützen.



Änderungen in Kapitel 4.2.1.3 SMB-Service

UnterA 25086-01 - Redirect zur Authentifizierung am TI-Gateway wird ergänzt:

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 parametrisiert 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.

[<=,]

A 25118 wird abgelöst durch

A_25118-01 -Authentisierungs-Endpunkt - Bereitstellung

Das Zugangsmodul MUSS einen Authentisierungs-Endpunkt bereitstellen und an diesem ausschließlich serverseitig authentifizierte https-Verbindungen zulassen. Das

Zugangsmodul MUSS anhand der Redirect_uri und des scope-Parameters ermitteln, ob ein HSM-B Bezug oder eine Cloud-PS-Anbindung autorisiert werden soll und die den TI-GW-Nutzer zur bestätigung der entsprechende Autorisierung auffordern.

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

unter A_25105 wird eingefügt.

A_28223 -Cloud-PS-Anbindung: Authentisierungs-Endpunkt - Auswertung Requests für Cloud-PS

Das Zugangsmodul MUSS die an seinem Authentisierungs-Endpunkt entsprechend A_28222 eingehenden Requests wie folgt verarbeiten:

- Prüfung, dass response_type = "code",
- Ermittlung von Cloud-PS (client_id), state, redirect_url und nonce für Verarbeitung entsprechend A_28224*,
- Prüfung, dass nonce nicht bereits für einen bestehenden aktuellen Auftrag des Cloud-PS (entsprechend client_id) verwendet wird (aktuell = innerhalb der Laufzeit einer nonce entsprechend A_28222),
- Prüfung, dass die redirect_uri der URL entspricht, die für dieses Cloud-PS konfiguriert ist.

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

unter A_25106 wird eingefügt

A_28224 -Cloud-PS-Anbindung: Authentisierungs-Endpunkt - Response im Erfolgsfall für Cloud-PS

Das Zugangsmodul MUSS genau nur wenn die Prüfungen in A_28223 positiv durchlaufen wurden

- dem Nutzer eine Login-Seite präsentieren, die eindeutig besagt, dass es um die Authentisierung im Zuge der Freigabe eines Cloud-PS geht und dabei den Namen des Cloud-PS anzeigen. Bei Mehrfachautorisationen (Liste der HSK-Instanzen abfragen, HSK-Instanz zur Nutzung freischalten, HSK-Instanz zur Konfiguration freischalten) müssen die Autorisierungen einzeln abgehakt werden.
- eine vollständige Nutzerauthentifizierung (siehe A_23242*) durchführen, eine bestehende Session darf also explizit nicht nachgenutzt werden, und
- im Erfolgsfall einen Authorization-Code erzeugen und intern verknüpft mit Name Cloud-PS, Gateway-UserID, Erstellungszeit und state, ablegen und
- den Nutzer wie folgt zum Cloud-PS zurückleiten:

HTTP/1.1 302 Found

Location: <redirect_uri>?code=<Authorization-Code>&state=<state>

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

A_25109 wird abgelöst durch

A_25109-01 -SMB-Service

Das Zugangsmodul MUSS einen Service-Endpunkt "SMB-Service" für den Austausch mit den Anbietern SMC-B und Cloud-PS anbieten. Das Zugangsmodul MUSS dabei durchsetzen, dass

- ausschließlich beidseitig authentifizierte TLS-Verbindungen genutzt werden,
- das Zugangsmodul als Serveridentität C.FD.TLS-S des TI-Gateway verwendet,
- ausschließlich Verbindungen von Clients akzeptiert werden, die sich mit einem C.FD.TLS-C eines Anbieters SMC-B (technische Rolle oid_anb_smcB) **oder einem konfigurierten Cloud-PS-Zertifikat** ausweisen (es gelten die Vorgaben aus gemSpec_Krypt für TLS Zertifikate) und
- das präsentierte TLS-Clientzertifikat, dem für den Anbieters SMC-B (TSPName/Name aus dessen TSL-Eintrag) **oder Cloud-PS (vereinbarter Name nach Formatvorgabe von A_27397)**, wie er entsprechend des innerhalb dieses TLS-Kanals empfangenen Requests identifiziert wurde (Client-ID), entspricht, wobei zur Prüfung auf die Daten entsprechend A_25103* **und die konfigurierten Cloud-PS** zurückgegriffen wird.

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

[A_25102 wird abgelöst durch](#)

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 • code ist ein noch gültiger vom Authentisierungs-Endpunkt des Zugangsmodul erzeugter Authorization-Code.
Verarbeitung	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.
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"

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

[unter A_25108 wird eingefügt](#)

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

Das Zugangsmodul 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": "<Access-Token>",
  "token_type": "bearer",
  "expires_in": 300,
  "id_token": "<ID-Token in JWS Compact Serialization>",
}
```

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

neue Operationsendpunkte:

A_26356 -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-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 access_token auf scope read:vKon 5. Rückmeldung an den Aufrufer
Rückgabe	Liste der HSK-Instanzen <pre>{ vkon: { name : "Name der HSK-Instanz" ; ip : "IP-Adresse der HSK-Instanz" } }</pre>
Fehlermeldung	to be done

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

A_28225 -Cloud-PS-Anbindung: Operation accessvKon

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

Service Endpunkt	<SMB-Service-URL>/accessvKon
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. 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	to be done

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

A_28226 -Cloud-PS-Anbindung: Operation restrictvKon

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	to be done

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

4 Änderung in gemILF_PS

Es wird Kapitel 3.5 neu aufgenommen

3.5 Direktanbindung von Cloud-Primärsystemen an das TI-Gateway

Neben Primärsystemen in der Umgebung des Leistungserbringers finden zunehmend auch Cloud-Primärsysteme (Cloud-PS) Verwendung, bei der die Leistung des Primärsystems als Service von einem Servicegeber bereitgestellt wird. Dabei wird das Primärsystem im Rechenzentrum des Servicegebers oder einem von ihm beauftragten Cloud-Plattform-Betreiber betrieben und von den Leistungserbringern über einen Webbrowser oder andere leichtgewichtige Clients genutzt. So ein Service kann von verschiedenen Leistungserbringerinstitutionen genutzt werden, die als Mandanten des Cloud-PS bezeichnet werden. Das Servicepersonal des Cloud-PS kann auch die Rolle eines DVO übernehmen.

A_26357 -TLS-Zertifikate mandantenspezifisch

Ein Cloud-PS MUSS für Verbindungen zu Konnektoren bzw. HSK-Instanzen für jeden seiner Mandanten ein eigenes TLS-Clientzertifikat verwenden. [≤,„]

A_26359 -Schutz privater Schlüssel

Ein Cloud-PS MUSS private Schlüssel entsprechend A_28203* sicher speichern und dabei gewährleisten, dass

- private Schlüssel für TLS-Clientzertifikate genau nur von den Cloud-PS-Kunden genutzt werden können, denen der Schlüssel gehört und
- das Auslesen privater Schlüssel ausgeschlossen ist und dabei explizit auch Zugriffsmöglichkeiten des Betriebspersonals der Cloud-Plattform berücksichtigen.

[≤,„]

A_26393 -Verbindung zur mandantenspezifischen Konnektor-Adresse

Ein Cloud-PS MUSS sicherstellen, dass seine Mandanten sich nur mit ihren eigenen Konnektoren bzw. HSK-Instanzen verbinden. HSK-Instanz-IP-Adressen müssen über die Operation requestvKon des TI-Gateways ermittelt werden und dürfen nicht manuell konfigurierbar sein. [≤,„]

A_26358 -TI-Zugang nur bei freigeschalteter SM-B

Ein Cloud-PS MUSS sicherstellen, dass einem Mandanten der Zugang zur TI nur ermöglicht wird, wenn der Nutzer des Mandanten seine Berechtigung durch Freischaltung einer SMC-B oder Aktivierung eines HSM-B nachgewiesen hat. [≤,„]

A_28346 -Zugriff nur durch Cloud-PS

Das Cloud-PS MUSS ausschließlich mit Anwendungen auf offene Fachdienste und WANDA zugreifen, dies es unter seine Kontrolle hat. Ein Netzwerkzugriff aus der Umgebungen seiner Mandanten über das Cloud-PS auf offene Fachdienste und WANDA ist ausgeschlossen. [≤,„]

A_26360 -CETP-Server mandantenspezifisch

Das Cloud-PS MUSS den CETP-Server mit mandantenindividuellem TLS-Server-Zertifikat betreiben. [≤,„]

Für Clientzertifikat (A_26357) und Serverzertifikat (A_26360) kann das gleiche Zertifikat verwendet werden.

Für den CETP-Client im HSK wird Server Name Indication eingeführt um diese Anforderung zu unterstützen. Mit der Anforderung soll verhindert werden, dass in vielen HSK-Instanzen das gleiche Clientzertifikat konfiguriert wird, um einen übergreifenden CETP-Server zu adressieren.

A_26441 -Rollentrennung beim Cloud-PS

Ein Cloud-PS MUSS sicherstellen, dass Mitarbeiter, die in der Rolle des DVO Konfigurationen an HSK-Instanzen vornehmen, keinen Zugang zu den Produktiven Interfaces (SOAP) der Konnektoren / HSK-Instanzen haben.

【<=,,】

Die Rollentrennung kann z.B. umgesetzt werden, dass Servicemitarbeiter über ein Netz als beauftragter DVO mit dem TI-Gateway verbunden sind und darüber die HSK-Instanzen konfigurieren, während das Cloud-PS über ein separates Netz, das als Cloud-PS beim TI-Gateway angeschlossen ist, auf die produktiven Interfaces des HSK-Instanzen zugreift.

A_26440 -Sichere Authentifizierung von Nutzer am Cloud-PS

Ein Cloud-PS MUSS seine Mandanten vor Zugriff auf das Cloud-PS sicher mittels Zwei-Faktor-Authentisierung (2FA) authentifizieren.【<=,,】